Network Checklist
V6R4

23 December 2005

Developed by DISA for the DOD

Database Reference Number: _____

Database entered by: _____ Date: _____

Technical Q/A by: _____Date: _____

Final Q/A by: _____ Date: _____

CAT I: _____

CAT II: _____

CAT III: _____

CAT IV: _____

Total: _____

FOUO UNTIL FILLED IN

CIRCLE ONE

FOR OFFICIAL USE ONLY (mark each page)

CONFIDENTIAL and SECRET (mark each page and each finding)

Classification is based on classification of system reviewed:

Unclassified System = FOUO Checklist
Confidential System = CONFIDENTIAL Checklist
Secret System = SECRET Checklist
Top Secret System = SECRET Checklist

Enclave Reviewer				**Phone**	
Previous SRR	Y N	**Date of Previous SRR**		**S01 Available**	Y N
Number of Current Open Findings					

Site Name	
Address	
Phone	

Position	**Name**	**Phone Number**	**Email**	**Area of Responsibility**
IAM				
IAO				

NET0090 CAT: 2 Network infrastructure is not properly documented.

Router Type:

Target(s): Router

8500.2 IA Control: DCHW-1: ECSC-1

Category: 12.9 - Documentation

Condition(s): Router

Vulnerability The IAO/NSO will maintain a current drawing of the site's network topology that includes all external and internal links, subnets, and all network equipment.

Vulnerability Discussion: To assist in the management, auditing, and security of the network infrastructure facility drawings and topology maps are a necessity. Topology maps are important because they show the overall layout of the network infrastructure and where devices are physically located. They also show the relationship and inter-connectivity between devices and where possible intrusive attacks (wire taps) could take place.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET Diagram: Validate the network diagram by correlating this information with all router and layer-3 switch configurations. Ensure that all subnets have been documented accordingly. To validate the connectivity as documented on the diagram, physically examine the cable connections for the downstream and upstream links as well as connections for major network components (JIDS, firewall, IDS, etc).

###Fixes###

NET Diagram: The NSO will maintain current up-to-date infrastructure and dataflow diagrams of the network under the NSO's control. The diagrams will include all remote connections, all local connections to domains not under site control, and all internal connections to PCs/workstations, servers, routers, bridges, and hubs or switches. This will help to show what the security, traffic, and physical impact of adding a new user(s) will be on the LAN. These diagrams will be based on a physical and if available an automated inspection of the network wiring plant. Special circumstances concerning the installation, such as a path that leaves a secure controlled environment, will be noted.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0130 CAT: 3 Network connections exist without approval

Router Type:

Target(s): Router

8500.2 IA Control: EBCR-1

Category: 12.2 - SSAA Doccumentation

Condition(s): Router

Vulnerability The IAO/NSO will ensure that all external connections are validated and approved prior to connection.

Vulnerability Discussion: A network is only as secure as its weakest link. It is imperative that all external connections be reviewed and kept to a minimum needed for operations. All external connections should be treated as untrusted networks. Reviewing who or what the network is connected to empowers the security manager to make sound judgements and security recommendations. Minimizing backdoor circuits and connections reduces the risk for unauthorized access to network resources.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET Circuit Apprv: Interview the IAM to verify that all connections have a mission requirement and that the DAA is aware of the requirement.

###Fixes###

NET Circuit Apprv: All external connections will be validated and approved prior to connection. Interview the IAM to verify that all connections have a mission requirement and that the DAA is aware of the requirement.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0135 CAT: 2 Unmanaged backdoor connections.

Router Type:

Target(s): Router

8500.2 IA Control: EBCR-1: ECSC-1

Category: 12.2 - SSAA Doccumentation

Condition(s): Router

Vulnerability The IAO/NSO will review all connection requirements on a semi-annual basis to ensure the need remains current, as well as evaluate all undocumented network connections discovered during inspections.

Vulnerability Discussion: A network is only as secure as its weakest link. It is imperative that all external connections be reviewed and kept to a minimum needed for operations. All external connections should be treated as untrusted networks. Reviewing who or what the network is connected to empowers the security manager to make sound judgements and security recommendations. Minimizing backdoor circuits and connections reduces the risk for unauthorized access to network resources.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET Circuit Review: Verify that the IAO/NSO is aware of all connections and has documented their reviews.

###Fixes###

NET Circuit Review: Verify the NSO is aware of all connections, and that all self-assessments require the NSO to verify the need for all connections.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0140 CAT: 3 Circuit location is not secure.

Router Type:

Target(s): Router

8500.2 IA Control: ECSC-1

Category: 14.5 - Physical Layer Security

Condition(s): Router

Vulnerability The IAO/NSO will ensure the connection between the CSU/DSU and the local exchange carrier's (LEC) data service jack (i.e., demarc) is in a secured environment.

Vulnerability Discussion: DOD leased lines carry an aggregate of sensitive and non-sensitive data; therefore unauthorized access must be restricted. Inadequate cable protection can lead to damage and denial of service attacks against the site and the LAN infrastructure.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET Comm Closet: The IAO/NSO will ensure the physical network components are in a secure environment.

###Fixes###

NET Comm Closet: The IAO will ensure all critical communicationsare in a controlled access areas. Controlled access area in this case means controlled restriction to authorize site personnel, i.e., dedicated communications rooms or locked cabinets. This is an area afforded entry control at a security level commensurate with the operational requirement. This protection will be sufficient to protect the network from unauthorized personnel. The keys to the locked cabinets and dedicated communications rooms will be controlled and only provided to authorized network/network security individuals.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0141 CAT: 3 The CSU\DSU modems are not disconnected.

Router Type:

Target(s): Router

8500.2 IA Control: ECSC-1

Category: 14.5 - Physical Layer Security

Condition(s): Router

Vulnerability The IAO/NSO will ensure the network management modems connected to all Channel Service Units (CSUs)/Data Service Units (DSUs) are disabled or disconnected when not in use.

Vulnerability Discussion: DOD leased lines carry an aggregate of sensitive and non-sensitive data; therefore: unauthorized access must be restricted. Inadequate cable protection can lead to damage and denial of service attacks against the site and the LAN infrastructure.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET CSU/DSU: Visually inspect the CSU\DSU to verify compliance.

###Fixes###

NET CSU/DSU: The IAO/NSO will ensure that network management modems connected to all Channel Service Units (CSUs)/Data Service Unite (DSUs) will be disabled or disconnecting when not in use.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0160 CAT: 1 A ISP connection exists without written approval.

Router Type:

Target(s): Router

8500.2 IA Control: EBCR-1: ECSC-1

Category: 12.6 - CAP

Condition(s): Router

Vulnerability The IAM will ensure that written approval is obtained from the GIG Waiver Panel or the Assistant Secretary of Defense (AS-NII) prior to establishing an ISP connection.

Vulnerability Discussion: A network is only as secure as its weakest link. It is imperative that all external connections be reviewed and kept to a minimum needed for operations. A connection to an ISP presents a greater risk to both the enclave as well as the entire NIPRNet. For this reason, ISP connections are prohibited unless a business case had been developed to justify the mission critical need for this connection and submitted to the GIG Waiver Panel to be reviewed and approved.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

Net ISP Unauthorized: Have the IAM provide a copy of the approval letter and then verify obtained from the GIG Waiver Panel or the Assistant Secretary of Defense (NII).

###Fixes###

NET ISP Unauthorized: Direct ISP connections are prohibited unless written approval is obtained from the GIG Waiver Panel or the ASD (NII). If this has not been done, a business case must be developed to justify the mission critical need for this connection and submitted to the GIG Waiver Panel to be reviewed and approved.Have the IAM provide a copy of the DAA written approval letter and then verify the mission need is still valid.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0162 CAT: 1 AG ingress ACL is not configured to secure enclave

Router Type:

Target(s): Router

8500.2 IA Control: ECSC-1

Category: 4.7 - Routers

Condition(s): Router

Vulnerability The IAO/NSO will ensure premise router interfaces that connect to an AG (i.e., ISP) are configured with an ingress ACL that only permits packets with destination addresses within the site's address space.

Vulnerability Discussion: Without verifying destination address of traffic coming from the sites AG, the premise router could be routing transit data from the Internet into the NIPRNet. This could also make the premise router vulnerable to a DoS attack as well as provide a backdoor into the NIPRNet.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET AG Ingress: Review the running config of the router that connects to an AG and verify that each permit statement of the ingress ACL is configured to only permit packets with destination addresses of the site's NIPRNet address space or that belonging to the address block assigned by the AG network service provider.

###Fixes###

NET AG Ingress: Insure the ingress ACL for any interface connected to an AAG is configured to only permit packets with a destination address belonging to the sites address block.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0164 CAT: 1 AG router has a routing protocol to the enclave.

Router Type:

Target(s): Router

8500.2 IA Control: ECSC-1

Category: 4.7 - Routers

Condition(s): Router

Vulnerability The IAO/NSO will ensure the premise router does not have a routing protocol session with a peer router belonging to an AS (Autonomous System) of the AG service provider.

Vulnerability Discussion: It would not be feasible to implement MD5 authentication with any BGP neighbors belonging to an ISP. Thus, this restriction will ensure that routing information shared by the BGP peers across the NIPRNet will not be corrupted through route updates sent from untrusted routers. By not redistributing NIPRNet routes into the ISP, unsolicited traffic that may inadvertently attempt to enter the NIPRNet by traversing the enclaves premise router will be avoided.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET AG Routes: Review the configuration of the router connecting to the AG and verify that there are no BGP neighbors whose remote AS belongs to the AG service provider.

###Fixes###

NET AG Routes: Use only a default static router to the AAG.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0166 CAT: 3 AG Network IP addresses are advertised in enclave

Router Type:

Target(s): Router

8500.2 IA Control: ECSC-1

Category: 4.7 - Routers

Condition(s): Router

Vulnerability The IAO/NSO will ensure the AG network service provider IP addresses are not redistributed into or advertised to the NIPRNet.

Vulnerability Discussion: By handling transit data from the NIPRNet to the sites AG, the additional workload on the router could place the device into a DoS state.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET AG IP Addresses: Review the configuration of the router connecting to the AG and verify that there are no BGP neighbors whose remote AS belongs to the AG service provider.

###Fixes###

NET AG IP Addresses: Use distribute lists prefix lists to insure AAG routes are not redistributed into the NIPRNet BGP or sites IGP (OSPF, EIGRP, RIP, etc).

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0170 CAT: 2 Backdoor network connections bypasses perimeter.

Router Type:

Target(s): Router

8500.2 IA Control: ECSC-1

Category: 12.6 - CAP

Condition(s): Router

Vulnerability The IAO/NSO will ensure that no backdoor connections exist between the site's secured private network and the Internet, NIPRNet, SIPRNet, or other external networks unless approved by the DAA.

Vulnerability Discussion: Backdoor connections allow for any individual or organization to possibly circumvent the Enclave Security Architecture and have unrestricted access into the network.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET Backdoor protection: Interview the IAM to verify that all connections have a mission requirement and that the DAA is aware of the requirement.

###Fixes###

NET Backdoor Protection: Backdoor connections that are not validated and approved by the CIO will be reported to the CIO for disposition.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0175 CAT: 1 The site is using IPv6 without DAA approval.

Router Type:

Target(s): Router

8500.2 IA Control: ECSC-1

Category: 12.4 - CM Process

Condition(s): Router

Vulnerability The IAO/NSO will ensure that IPv6 implemented on any DOD network that transports production or operations traffic is approved by the DAA.

Vulnerability Discussion: As part of the GIG integrated architecture strategy, the migration to IPv6 across DoD networks will consider operational requirements, risks, and costs, while maintaining interoperability within the DoD, across the Federal Government, and among business partners in the commercial sector. It is mandated the internetworking protocol version 6 be approved by the DAA..

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET IPv6 Approval: Review all router configurations to determine if they have been enabled to forward IPv6 unicast datagrams and if any IPv6 addresses have been assigned to any interfaces.

###Fixes###

NET IPv6 Approval: Ensure that all IPv6 migrations plans are approved by the DAA prior to implementation on production or operational networks.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0180 CAT: 2 Non-registered or unauthorized IP addresses.

Router Type:

Target(s): Router

8500.2 IA Control: ECSC-1

Category: 12.4 - CM Process

Condition(s): Router

Vulnerability The IAO/NSO will ensure all network IP address ranges are properly registered with the .MIL Network Information Center (NIC).

Vulnerability Discussion: Allowing subscribers onto the network whose IP addresses are not registered with the .Mil NIC may allow unauthorized users access into the network. These unauthorized users could then monitor the network, steal passwords, and access classified information.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET Registered IP Address: Connect via the web to www.nic.mil, and click on search whois under DISN services. Enter the first three octets of the local site IP range into the keyword search section and then select all categories and submit the request. Verify that the site is registered for the range.

###Fixes###

NET Registered IP Address: The IAO will ensure all users accessing the network have a legitimate need and will submit any unregistered IP addresses to the .Mil Network Information Center (NIC) for registration.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0185 CAT: 2 Unauthorized addresses within Siprnet enclave

Router Type:

Target(s): Router

8500.2 IA Control: ECSC-1

Category: 12.4 - CM Process

Condition(s): Router

Vulnerability The IAO/NSO will ensure that all addresses used within the site's SIPRNet infrastructure are authorized .mil addresses that have been registered and assigned to the activity. RFC1918 addresses are not permitted.

Vulnerability Discussion: If network address space is not properly configured, managed, and controlled, the network could be accessed by unauthorized personnel resulting in security compromise of site information and resources.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET Sipr RFC1918: Inspect the network topology diagrams as well as all configured router interfaces to determine what addresses are being utilized. Private addresses in accordance with RFC 1918 are not permitted within the SIPRNet enclave.

###Fixes###

NET Sipr RFC1918: The IAO will ensure that the site uses only authorized .mil addresses that have been registered and assigned to the activity for the SIPRNet.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0186 CAT: 2 Advertising unauthorized addresses into NIPRNET

Router Type:

Target(s): Router

8500.2 IA Control: ECSC-1

Category: 4.7 - Routers

Condition(s): Router

Vulnerability The Router Administrator will block all BOGON / Martian, and private IP addresses from traversing the IP WAN. The Router Administrator will have a procedure in place to check for changes and modify the BOGON/Martian list on a monthly basis.

Vulnerability Discussion: If network address space is not properly configured, managed, and controlled, the network could be accessed by unauthorized personnel resulting in security compromise of site information and resources.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET Route Advertisements: Inspect the router's ACLs against the Appendix C and ensure they are applied to the interface. The router administrator will have a procedure in place to change or modify the BOGON/Martian list on a monthly basis.

###Fixes###

NET Route Advertisements: The IAO/NSO will ensure that the site uses only authorized .mil addresses that have been registered and assigned to the activity for advertisements.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0190 CAT: 3 LAN addresses are not protected from the public.

Router Type:

Target(s): Router

8500.2 IA Control: ECSC-1

Category: 12.4 - CM Process

Condition(s): Router

Vulnerability The IAO/NSO will ensure that workstation clients' real addresses are not revealed to the public by implementing NAT on the firewall or the router.

CAVEAT: If the site has implemented an application-level firewall, hiding of the clients' real address can also be done by enabling the proxies to replace the clients' real source address with that of the firewall's external IP address or an address from a NAT pool.

Mark this as N/A for SIPRNet Enclaves that are not implementing NAT. If the site has implemented NAT on the SIPR, it must be a static one-to-one NAT to a real, smil.mil assigned IP address (no RFC 1918 addresses).

Vulnerability Discussion: An attacker can learn more about a sites private network once it has discovered the real IP addresses of the hosts within.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET NAT Requirement: Review the firewall or premise router configuration to determine if NAT has been implemented.

###Fixes###

NET NAT Requirement: Implement Network Address Translation (NAT) on the firewall or premise router for NIPRNet Enclaves.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0198 CAT: 3 The DHCP server is not configured to log hostnames

Router Type:

Target(s): Router

8500.2 IA Control: ECSC-1

Category: 10.5 - Retention

Condition(s): Router

Vulnerability The IAO/NSO will ensure that the DHCP server is configured to log hostnames or MAC addresses for all clients and all logs are stored online for 30 days and offline for one year.

Vulnerability Discussion: In order to identify and combat IP address spoofing, it is highly recommended that the DHCP server logs MAC addresses or hostnames on the DHCP server.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET DHCP Logging: Have the DHCP administrator display the log files for visual inspection. Verify retention of log files.

###Fixes###

NET DHCP Logging: The IAO will ensure that the DHCP server is configured to log hostnames or MAC addresses.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0199 CAT: 3 DHCP lease duration is less than 30 days on SIPR.

Router Type:

Target(s): Router

8500.2 IA Control: ECSC-1

Category: 14.3 - Network Device Configuration

Condition(s): Router

Vulnerability The IAO/NSO will ensure that any DHCP server used within SIPRNet infrastructure is configured with a lease duration time of 30 days or more.

Vulnerability Discussion: In order to trace, audit, and investigate suspicious activity, DHCP servers within the SIPRNet infrastructure must have the minimum lease duration time configured to 30 or more days.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET DHCP Lease Duration: Review the DHCP configuration.

###Fixes###

NET DHCP Lease Duration: The IAO will ensure that any DHCP server used within SIPRNet infrastructure is configured with a minimum duration time of the lease to 30 or more days.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0210 CAT: 2 Network devices are not stored in secure Comm room

Router Type:

Target(s): Router

8500.2 IA Control: ECSC-1

Category: 5.9 - Device Locations

Condition(s): Router

Vulnerability The IAO/NSO will ensure that all network devices (i.e., IDS, routers, RAS, NAS, firewalls, etc.) are located in a secure room with limited access.

Vulnerability Discussion: If all communications devices are not installed within controlled access areas, risk of unauthorized access and equipment failure exists, which could result in denial of service or security compromise. It is not sufficient to limit access to only the outside world or non-site personnel. Not everyone with the site has the need-to-know or the need-for-access to communication devices.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET Comm Closet: The IAO/NSO will ensure the physical network components are in a secure environment.

###Fixes###

NET Comm Closet: The IAO will ensure all critical communicationsare in a controlled access areas. Controlled access area in this case means controlled restriction to authorize site personnel, i.e., dedicated communications rooms or locked cabinets. This is an area afforded entry control at a security level commensurate with the operational requirement. This protection will be sufficient to protect the network from unauthorized personnel. The keys to the locked cabinets and dedicated communications rooms will be controlled and only provided to authorized network/network security individuals.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0230 CAT: 1 Communications devices are not password protected.

Router Type:

Target(s): Router

8500.2 IA Control: ECSC-1

Category: 1.3 - Identity Management

Condition(s): Router

Vulnerability The IAO/NSO will ensure all communications devices are password protected.

Vulnerability Discussion: The lack of a password protection for communications devices provides anyone access to the device, which opens a backdoor opportunity for intruders to attack and manipulate or compromise network resources. Vendors and programmers often leave methods of gaining access to a device that is outside the normal means of access. These backdoors or hidden userids are well known and are extremely dangerous if left active.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET Password Protection: Interview the network administrator and attempt to logon to several devices.

###Fixes###

NET Password Protection: Ensure all communication devices are in compliance with password policy.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0240 CAT: 1 Devices exist that have standard default passwords

Router Type:

Target(s): Router

8500.2 IA Control: ECSC-1

Category: 1.3 - Identity Management

Condition(s): Router

Vulnerability The IAO/NSO will ensure all default manufacturer passwords are changed.

Vulnerability Discussion: Devices not protected with strong password schemes provide the opportunity for anyone to crack the password thus gaining access to the device and causing network, device, or information damage, or denial of service. Not changing the password in a timely manner increases the likelihood that someone will capture or crack the password and gain unauthorized access to the device.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET Password Protection: Interview the network administrator and attempt to logon to several devices.

###Fixes###

NET Password Protection: Ensure all communication devices are in compliance with password policy.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0260 CAT: 2 Accepted password generation schemes are not used.

Router Type:

Target(s): Router

8500.2 IA Control: ECSC-1

Category: 1.1 - Passwords

Condition(s): Router

Vulnerability The IAO/NSO will ensure all passwords are created and maintained in accordance with the rules outlined in DODI 8500.2, IAIA-1, and IAIA-2. http://www.dtic.mil/whs/directives/corres/html/85002.htm.

Vulnerability Discussion: Devices protected with weak password schemes provide the opportunity for anyone to crack the password, gaining access to the device and causing network, device, or information damage or denial of service.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET Password Protection: Interview the network administrator and attempt to logon to several devices.

###Fixes###

NET Password Protection: Ensure all communication devices are in compliance with password policy.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0270 CAT: 2 Passwords are not recorded and stored properly.

Router Type:

Target(s): Router

8500.2 IA Control: DCBP-1: ECSC-1

Category: 1.6 - Documentation and Storage

Condition(s): Router

Vulnerability The IAO/NSO will record the locally configured passwords used on communications devices and store them in a secured manner.

Vulnerability Discussion: Passwords should be recorded and stored in a secure location for emergency use. This helps prevent time consuming password recovery techniques and denial of administrator access, in the event a password is forgotten or the individual with the access is incapacitated. Router configurations contain passwords in clear text. This must be encrypted for use in areas where this can be compromised.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET PSWD Recorded/Stored: Passwords need to be recorded and stored in a secure manner.

###Fixes###

NET PSWD Recorded/Stored: The IAO will record the passwords used on communications devices and store them in a secure or controlled manner.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0280 CAT: 3 Integrity of image files loaded

Router Type:

Target(s): Router

8500.2 IA Control: COBR-1

Category: 8.6 - Object Integrity

Condition(s): Router

Vulnerability The IAO/NSO will ensure that a documented procedure is in place to validate loaded image files, and that they are checked on a monthly basis to ensure the file has not been corrupted or altered.

Vulnerability Discussion: It is important that image files can only be downloaded or uploaded from authorized computers. Restricting the IP address of the image server will lessen the possibility of someone uploading an invalid image file. Automated configuration reloads without integrity checks can lead to denial-of-service, sniffer attacks, and undetected network vulnerabilities. Protecting the configuration or image file while stored on a computer ensures a bogus copy or Trojan horse version has not been put in its place.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET Data at Rest: Network data at rest needs to be periodically reviewed for it's integrity content.

###Fixes###

NET Data at Rest: Ensure network data is checked on a monthly basis to ensure the data has not been corrupted or altered. Store files in a secure manner and validate monthly to protect against unauthorized manipulation and corruption.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0300 CAT: 2 Disable unused ports and services.

Router Type:

Target(s): Router

8500.2 IA Control: ECSC-1

Category: 14.5 - Physical Layer Security

Condition(s): Router

Vulnerability The IAO/NSO will disable all network management ports and services except those needed to support the operational commitments of the site.

Vulnerability Discussion: Allowing excessive or non-required ports, whether virtual (such as ECHO or CHARGEN) or physical (such as console or modem), to remain active provides one more point of attack for unauthorized personnel to exploit. Care should be taken in disabling AUX ports because a site may lock themselves out of a device. Direct connection management ensures the passwords are not transmitted in clear text over vulnerable LANs and ensures the site has a method of accessing the devices should the virtual ports be inaccessible due to attacks. Digital signatures allows accurate auditing and identification of personnel performing the management functions.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET Unused Ports/Services: Interview the IAO/NSO and Network Administrator to determine operation requirements then review the configuration of the device.

###Fixes###

NET Unused Ports/Services: The IAO will ensure all ports and services except those needed to support the operational commitments of the site are disabled.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0310 CAT: 2 Out-of-band required for network management.

Router Type:

Target(s): ACE Server; Collaboration Gateway; FTP Server; Load Balancer/

8500.2 IA Control: EBRP-1: ECSC-1: IAIA-1: IAIA-2

Category: 14.1 - Network Management Services (NMS)

Condition(s): RADIUS Server: ACE Server: TACACS+ Server: TFTP Server: Syslog Server: Remote Access Server: Proxy Server/Gateway Server: Network/Element Management Server: Mail Gateway: Load Balancer/Content Switch: Collaboration Gateway: FTP Server

Vulnerability The IAO/NSO will ensure all communication. Device management utilizes the OOB or direct connection method for communications device management is used.

To ensure the proper authorized network administrator is the only one who can access the device, the IAO/NSO will ensure OOB access enforces the following security restrictions:

- Two-factor authentication (e.g., Secure ID, DOD PKI)
- Encryption of management session (FIPS 140-2 validated encryption)
- Auditing

Vulnerability Discussion: Without secure out-of-band management implemented with authenticated access controls, strong two-factor authentication, encryption of the management session and audit logs, unauthorized users may gain access to network managed devices such as routers or communications servers (CSs). If the router network is compromised, large parts of the network could be incapacitated with only a few commands. If a CS is compromised, unauthorized users could gain access to the network and its attached systems. The CS could be disabled, therefore disallowing authorized subscribers from supporting mission critical functions.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET OOB Two-factor requirement: Interview the IAO/NSO to determine if the site is compliant with this requirement.

First review the device configuration to first ensure that an authentication server is being used. Then verify that a 2-factor authentication method has been implemented.

###Fixes###

NET OOB Two-factor requirement: The network administrator will manage devices through out-of-band or direct connection. In-band management of network devices will be limited to situations where out-of-band management would hinder operational commitments or when emergency situations arise.

The router administrator will configure the router to utilize the most currently supported version of SSH with all security patches applied.

If the direct connection method is impractical, the dial-up method is the next best alternative. The dial-up method will utilize secure dial-up into a TACACS+ server inside the enclave via an encryption utility.

The network administrator will configure the routers to ensure authenticated access control, strong two-factor authentication, encryption of the management session and audit logs are all being incorporated in the access scheme, when out of band (e.g., dial-up) management is necessary.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0320 CAT: 2 Use of in-band management is not limited.

Router Type:

Target(s): ACE Server; Collaboration Gateway; FTP Server; Load Balancer/

8500.2 IA Control: DCBP-1: ECND-1: ECND-2: ECSC-1

Category: 14.1 - Network Management Services (NMS)

Condition(s): Collaboration Gateway: TACACS+ Server: Syslog Server: Remote Access Server: RADIUS Server: Proxy Server/Gateway Server: Network/Element Management Server: Mail Gateway: FTP Server: TFTP Server: ACE Server: Load Balancer/Content Switch

Vulnerability The network administrator will limit the use of in-band management to situations where the use of OOB management would hinder operational commitments or when emergency situations arise. The IAO/NSO will approve the use of in-band management on a case-by-case documented basis.

Vulnerability Discussion: It is imperative that communications used for administrative access to network components is limited to emergency situations or where out-of-band management would hinder daily operational requirements. In-band management introduces the risk of an attacker gaining access to the network internally or even externally.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET In-band limited: Interview the IAO/NSO for compliance. Ask to see documentation.

###Fixes###

NET In-band limited: Use out-of-band management.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0322 CAT: 2 Two-factor authentication is not used.

Router Type:

Target(s): ACE Server; Collaboration Gateway; FTP Server; Load Balancer/

8500.2 IA Control: ECSC-1: IAIA-1: IAIA-2

Category: 1.4 - Authentication Services

Condition(s): Syslog Server: TACACS+ Server: Proxy Server/Gateway Server: Remote Access Server: RADIUS Server: Mail Gateway: Load Balancer/Content Switch: FTP Server: Collaboration Gateway: ACE Server: TFTP Server: Network/Element Management Server

Vulnerability For in-band management, the IAO/NSO will implement the use of strong two-factor authentication for all access to all communications devices.

Vulnerability Discussion: Without strong two-factor authorization, unauthorized users may gain access to network managed devices such as routers, firewalls, remote access servers, etc. If any of these devices are compromised, the entire network could also be compromised.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET In-band Two-factor: First review the device configuration to first ensure that an authentication server is being used. Then verify that a 2-factor authentication method has been implemented.

###Fixes###

NET In-band Two-factor: The network device and authentication servers will be configured so that all authorized users are forced to use two-factor authentication.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0324 CAT: 2 In-band management is not restricted.

Router Type:

Target(s): ACE Server; Collaboration Gateway; FTP Server; Load Balancer/

8500.2 IA Control: ECND-1: ECND-2: ECSC-1

Category: 14.3 - Network Device Configuration

Condition(s): Mail Gateway: TFTP Server: TACACS+ Server: Syslog Server: Remote Access Server: RADIUS Server: Network/Element Management Server: Load Balancer/Content Switch: FTP Server: Collaboration Gateway: ACE Server: Proxy Server/Gateway Server

Vulnerability The IAO/NSO will ensure that the use of in-band management is restricted to a limited number of authorized IP addresses. The number of IP addresses must be equal to or less than the number of network administrator.

Vulnerability Discussion: Without limited in-band management connections, unauthorized users may gain access to network managed devices such as routers, firewalls, remote access servers, etc. If any of these devices are compromised, the entire network could also be compromised.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET In-band LAN Restricted: Examine all network components (i.e., router, switch, firewall, NAS) configurations to determine what IP addresses are permitted access via telnet or SSH. If a terminal server is used, you will need to review that configuration as well.

###Fixes###

NET In-band LAN Restricted: For in-band management, the router administrator will configure the network device to restrict the use of in-band connections to a limited number (less than 10) of authorized IP addresses.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0326 CAT: 2 In-band management requires encryption.

Router Type:

Target(s): ACE Server; Collaboration Gateway; FTP Server; Load Balancer/

8500.2 IA Control: ECNK-1: ECSC-1

Category: 8.1 - Encrypted Data in Transit

Condition(s): RADIUS Server: FTP Server: TFTP Server: TACACS+ Server: Syslog Server: Remote Access Server: Network/Element Management Server: Load Balancer/Content Switch: Mail Gateway: Collaboration Gateway: ACE Server: Proxy Server/Gateway Server

Vulnerability The IAO/NSO will ensure in-band management access to a network device is secured using FIPS 140-2 validated encryption such as AES, 3DES, SSH, or SSL.

Vulnerability Discussion: Without encrypted in-band management connections, unauthorized users may gain access to network managed devices such as routers, firewalls, remote access servers, etc. If any of these devices are compromised, the entire network could also be compromised. Administrative access requires the use of encryption on all communication channels between the remote user and the system being accessed. It is imperative to protect communications used for administrative access as an attacker manages to hijack the link would gain immediate access to the network.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET In-band FIPS 140-2: Procedure: Examine network components (i.e., NAS) configurations for use of validated encryption.

###Fixes###

NET In-band FIPS 140-2: For in-band management, the router administrator will configure the network device to only allow SSH connections.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0340 CAT: 2 Warning banner compliance to 8500.2 ECWM-1.

Router Type:

Target(s): Router

8500.2 IA Control: ECWM-1

Category: 11.6 - Warning Banners

Condition(s): Router

Vulnerability The IAO/NSO will ensure warning banners are deployed on all network devices allowing SSH, Telnet, File Transfer Protocol (FTP), or Hyper-Text Transfer Protocol (HTTP) access in accordance with DODI 8500.2 ECWM-1.

Vulnerability Discussion: Failure to display the required login banner prior to logon attempts will limit the sites ability to prosecute unauthorized access and also presents the potential to give rise to criminal and civil liability for systems administrators and information systems managers. Not displaying the proper banner will also hamper the sites ability to monitor device usage.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET Warning Banners: Have the network administrators sign onto each managed network device to ensure the DoD approved warning banners are displayed before the password prompt and after a correct login.

###Fixes###

NET Warning Banner: Display the approved DOD login banner prior to a login attempt on all network devices allowing Telnet, File Transfer Protocol (ftp), or Hyper Text Transfer Protocol (http) access.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0400 CAT: 2 Router neighbor authentication with MD5 required.

Router Type: All Routers

Target(s): Router

8500.2 IA Control: ECSC-1

Category: 1.4 - Authentication Services

Condition(s): Router

Vulnerability The router administrator will ensure neighbor authentication with MD5 is implemented for all routing protocols with all peer routers within the same or between autonomous systems (AS).

CAVEAT: Neighbor router authentication will not be required between the site's premise router and a NIPRNet or SIPRNet subscriber interface on the hub router.

Vulnerability Discussion: Routing protocols should use MD5 to authenticate neighbors prior to exchanging route table updates to ensure that route tables are not corrupted.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET MD5 Authentication: Procedure: Reference the appropriate router checklist procedure guide.

###Fixes###

NET MD5 Authentication: The router administrator will configure the routers so that MD5 authentication is used to authenticate routing protocol neighbors.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0410 CAT: 2 BGP sessions are not restricted.

Router Type: Premise Routers
Target(s): Router
8500.2 IA Control: ECSC-1
Category: 4.7 - Routers
Condition(s): Router

Vulnerability The router administrator will restrict BGP connections to known IP addresses of neighbor routers from a trusted AS.

Vulnerability Discussion: BGP routers will only establish sessions with neighbors that have been configured. However, as an additional safety net, use filtering of BGP connections based on source address and only allow those connections to the premise router.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET BGP Route Filtering: Procedure: Reference the appropriate router checklist procedure guide.

###Fixes###

NET BGP Route Filtering: The router administrator will create ingress ACL to block any unauthorized BGP connection attempts.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0420 CAT: 3 Procedures and maintenance for MD5 keys

Router Type: All Routers
Target(s): Router
8500.2 IA Control: IAKM-1: IAKM-2: IAKM-3
Category: 12.9 - Documentation
Condition(s): Router

Vulnerability The IAO/NSO will ensure there are written procedures for MD5 key management to include: key exchange, storage, and expiration. Keys will be changed every six months.

Vulnerability Discussion: MD5 is a public key encryption algorithm which uses the exchange of encryption keys across a network link. If these keys are not managed properly, they could be intercepted by unauthorized users and used to break the encryption algorithm.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET MD5 Key Management: Review the site's written procedures.

###Fixes###

NET MD5 Key Management: The IAO will ensure that written procedures are available for MD5 overall key management on the network. Areas of management that will be included are key exchange, time expiration, physical storage and key compromise.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0425 CAT: 1 MD5 Key Lifetime expiration is set to never expire

Router Type: All Routers

Target(s): Router

8500.2 IA Control: ECSC-1

Category: 4.7 - Routers

Condition(s): Router

Vulnerability The IAO/NSO will ensure the lifetime of a MD5 Key expiration is set to never expire. The lifetime of the MD5 key will be configured as infinite for route authentication, if supported by the current approved router software version.

Note: Only Enhanced Interior Gateway Routing Protocol (EIGRP), and Routing Information Protocol (RIP) Version 2 use key chains.

Vulnerability Discussion: This check is in place to ensure keys do not expire creating a DOS due to adjacencies being dropped and routes being aged out. The recommendation is to use two rotating six month keys with a third key set as infinite lifetime. The lifetime key should be changed 7 days after the rotating keys have expired and redefined.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

IOS Procedure: Reference the CISCO router checklist procedure guide.

JUNOS Procedure: This is NA for Juniper routers.

###Fixes###

NET MD5 Lifetime Key: This check is in place to ensure keys do not expire creating a DOS due to adjacencies being dropped and routes being aged out. The recommendation is to use two rotating six month keys with a third key set as infinite lifetime. The lifetime key should be changed 7 days after the rotating keys have expired and redefined.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0430 CAT: 2 Authentication server used to gain access

Router Type: All Routers

Target(s): Router

8500.2 IA Control:

Category: 1.4 - Authentication Services

Condition(s): Router

Vulnerability The IAO/NSO will ensure an authentication server is used to gain administrative access to all routers.

Vulnerability Discussion: Without TACACS+ and AAA, unauthorized users may gain access and possibly control of the routers. If the router network is compromised, large portions of the network could be incapacitated with only a few commands.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET Authentication Access: Procedure: Reference the appropriate router checklist procedure guide.

###Fixes###

NET Authentication Access: The router administrator will configure the TACACS+ server with standard accounts and user passwords. The router administrator will ensure that standard accounts are not created directly on the router. The router administrator will ensure that the site uses RADIUS, TACACS+, or other DOD approved device for remote administrative access to the router.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0440 CAT: 2 Emergency accounts limited to one.

Router Type:	All Routers	Target(s):	Router
8500.2 IA Control:	ECSC-1	Category:	1.3 - Identity Management
Condition(s):	Router		

Vulnerability The IAO/NSO will ensure when an authentication server is used for administrative access to the router, only one account is defined locally on the router for use in an emergency (i.e., authentication server or connection to the server is down).

Vulnerability Discussion: Authentication for administrative access to the router is required at all times. A single account can be created on the routers local database for use in an emergency such as when the authentication server is down or connectivity between the router and the authentication server is not operable.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET Emergency Account: IOS Procedure: Review the running configuration and verify that only one local account has been defined. Example: username xxxxxxx password 7 xxxxxxxxxxx

Junos Procedure: Reference the Juniper router checklist procedure guide.

###Fixes###

NET Emergency Account: Insure that only one local account has been defined on the router and store the username and password in a secured manner.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0460 CAT: 1 Group accounts or user accounts without passwords

Router Type: All Routers

Target(s): Router

8500.2 IA Control: IAIA-1: IAIA-2

Category: 1.3 - Identity Management

Condition(s): Router

Vulnerability The router administrator will ensure each user has their own account to access the router with username and password.

Vulnerability Discussion: Without passwords on user accounts, one level of complexity is removed from gaining access to the routers. If a default userid has not been changed or is guessed by an attacker, the network could be easily compromised as the only remaining step would be to crack the password.

Sharing group accounts on any router is strictly prohibited. If these group accounts are not changed when someone leaves the group, that person could possibly gain control of the router. Having group accounts does not allow for proper auditing of who is accessing or changing the network.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET Group Accounts: Review router configuration for local accounts defined to router. If an authentication server is being used, examine those accounts with access to the routers.

###Fixes###

NET Group Accounts: The router administrator will ensure that all user accounts without passwords are removed.

The router administrator will ensure that individual user accounts are created for each authorized router administrator. The IAO will ensure that any group or duplicate account will be removed.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0465 CAT: 2 Assign lowest privilege level to user accounts.

Router Type: All Routers

Target(s): Router

8500.2 IA Control: ECSC-1

Category: 2.2 - Least Privilege

Condition(s): Router

Vulnerability The router administrator will ensure all user accounts are assigned the lowest privilege level that allows them to perform their duties.

Vulnerability Discussion: By not restricting router administrators to their proper privilege levels, access to restricted functions may be allowed before they are trained or experienced enough to use those functions. Network disruptions or outages could be caused by mistakes made by inexperienced administrators.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET Lowest Privilege Level: Reference the appropriate router checklist procedure guide.

###Fixes###

NET Lowest Privilege Level: The router administrator will assign router accounts with the least privilege rule. Each user will have access to only the privileges they require to perform their respective duties. Access to the highest privilege levels should be restricted to a few users.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0470 CAT: 2 Unnecessary or unauthorized router accounts exist.

Router Type: All Routers
Target(s): Router
8500.2 IA Control: ECSC-1
Category: 1.3 - Identity Management
Condition(s): Router

Vulnerability The router administrator will immediately remove accounts from the authentication server or router that are no longer required.

Vulnerability Discussion: Allowing unnecessary or unauthorized accounts may allow for them to be compromised by unauthorized users who could then gain full control of the router. Denial of service, interception of sensitive information or other destructive actions could then take place.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET Account Administration: Verify that the site is in compliance by reviewing site's responsibilities list and reconcile this list with those accounts defined locally or in the authentication server.

###Fixes###

NET Account Administration: The administrator will ensure that procedures are in place to enforce proper account administration. The administrator will ensure that any account that is no longer needed will be disabled or removed from the system.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0580 CAT: 3 Password required on the JUNOS diagnostic port.

Router Type: All Routers
Target(s): Router
8500.2 IA Control: IAIA-1: IAIA-2
Category: 1.3 - Identity Management
Condition(s): Router

Vulnerability The router administrator will ensure a password is required to gain access to the router's diagnostics port.

Vulnerability Discussion: If unauthorized users gain access to the routers diagnostic port, it is possible to disrupt service.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET JUNOS Diagnostic Port: IOS Procedure: N/A A Cisco router does not have a diagnostics port.

JUNOS Procedure: Review the router configuration to ensure a password is required when gaining access to the diagnostics port similar to the following:

```
[edit system]
diag-port-authentication {
  encrypted-password "xxxxxxxxxxxx"; # SECRET-DATA
}
```

###Fixes###

NET JUNOS Diagnostic Port: The router administrator will ensure that a password is required to access the routers diagnostic port.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0590 CAT: 3 Enable secret passwords are not unique.

Router Type: All Routers

Target(s): Router

8500.2 IA Control: IAIA-1: IAIA-2

Category: 1.3 - Identity Management

Condition(s): Router

Vulnerability The router administrator will ensure the enable secret password does not match any other username password, enable password, or any other enable secret password.

Vulnerability Discussion: Without unique enable secret passwords on each router, the chance that a password will be compromised is increased. If an employee is terminated or leaves employment for another reason, if the password they are familiar with is changed on one router, it may still exist on other routers. This may lead to an increased ability to compromise the remaining routers. Denial of service, interception of sensitive information, or other destructive actions could take place.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET Enable Secret Unique: IOS Procedure: Interview the router administrators to see if this is being enforced on all Cisco routers.

JUNOS Procedure: This is NA for Juniper routers as there is no enable mode passwords—that is, there is no password prompt to enter edit or configuration mode.

###Fixes###

NET Enable Secret Unique: The router administrator will configure each router with a unique enable secret password and remove all others.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0600 CAT: 2 Passwords are viewable when displaying the router

Router Type: All Routers

Target(s): Router

8500.2 IA Control: ECSC-1

Category: 1.6 - Documentation and Storage

Condition(s): Router

Vulnerability The router administrator will ensure passwords are not viewable when displaying the router configuration. Type 5 encryption must be used for the enable mode password (i.e., enable secret password).

Vulnerability Discussion: Many attacks on DOD computer systems are launched from within the network by unsatisfied or disgruntled employees, therefore, it is imperative that all router passwords are encrypted so they cannot be intercepted by viewing the console. If the router network is compromised, then large parts of the network could be incapacitated with only a few commands.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET Type 5 encryption: IOS Procedure: Examine all Cisco router configurations to determine if the global command service password-encryption is present.

JUNOS Procedure: For JUNOS, all passwords are always shown as encrypted; hence, this would never be a finding.

###Fixes###

NET Type 5 encryption: The router administrator will configure each router using the service password encryption option. Service password-encryption is the required global config mode command.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0630 CAT: 3 Device management is not using a OOB network.

Router Type: All Routers

Target(s): Router

8500.2 IA Control: ECSC-1

Category: 4.7 - Routers

Condition(s): Router

Vulnerability The IAO/NSO will ensure route management utilizes the OOB or direct connection method for communications device management.

Vulnerability Discussion: From an architectural point of view, providing Out-Of-Band (OOB) management of network systems is the best first step in any management strategy. No production traffic resides on an out-of-band network.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET OOB Management: Interview the IAO/NSO to determine if the site is compliant with this requirement.

###Fixes###

NET OOB Management: The network administrator will manage devices through out-of-band or direct connection. If the direct connection method is impractical, the dial-up method is the next best alternative. The dial-up method will utilize secure dial-up into a TACACS+ server inside the enclave via an encryption utility. The network administrator will configure the routers to ensure authenticated access control, strong two-factor authentication, encryption of the management session and audit logs are all being incorporated in the access scheme, when out of band (e.g., dial-up) management is necessary.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0640 CAT: 2 Two-factor authentication, encryption required.

Router Type:	All Routers	Target(s):	Router
8500.2 IA Control:	ECSC-1	Category:	1.1 - Passwords
Condition(s):	Router		

Vulnerability To ensure the proper authorized network administrator is the only one who can access the device, the IAO/NSO will ensure OOB access enforces the following security restrictions:

- Two-factor authentication (e.g., Secure ID, DOD PKI)
- Encryption of management session (FIPS 140-2 validated encryption)
- Auditing

Vulnerability Discussion: Without secure out-of-band management implemented with authenticated access controls, strong two-factor authentication, encryption of the management session and audit logs, unauthorized users may gain access to network managed devices compromised, large parts of the network could be incapacitated with only a few commands.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

Net Two-factor Authentication: First review the device configuration to ensure that an authentication server is being used. Then verify that a 2-factor authentication method has been implemented.

###Fixes###

NET Two-factor Authentication: The router administrator will configure the router to utilize the most currently supported version of SSH with all security patches applied. The network administrator will configure the routers to ensure authenticated access control, strong two-factor authentication, encryption of the management session and audit logs are all being incorporated in the access scheme.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0645 CAT: 1 Routers are not password protected for out-of-band

Router Type: All Routers
Target(s): Router
8500.2 IA Control: IAIA-1: IAIA-2
Category: 1.3 - Identity Management
Condition(s): Router

Vulnerability The IAO/NSO will ensure that all OOB management connections to the router require passwords.

Vulnerability Discussion: Devices protected with weak password schemes or no password at all, provide the opportunity for anyone to crack the password or gain access to the device and cause network, device, or information damage or denial of service.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET OOB PSW Protected: IOS Procedure: The console port and the vty ports used by the OOBM network should look similar to the following:
login authentication admin_only
exec-timeout 10 0
transport input ssh

JUNOS Procedure: Any access to a Juniper router requires a login. You can not use CLI unless you are logged in; hence, this will never be a finding.

###Fixes###

NET OOB PSW Protected: The site will ensure that all out-of-band management connections to the router have passwords.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0650 CAT: 2 Console port is not configured to timeout-10 min

Router Type: All Routers
Target(s): Router
8500.2 IA Control: ECSC-1
Category: 4.7 - Routers
Condition(s): Router

Vulnerability The router administrator will ensure the router console port is configured to time out after 10 minutes or less of inactivity.

Vulnerability Discussion: Routers have multiple areas of configuration. The more critical the area, the tighter the control should be. Setting the timeout of the session to fifteen minutes or less increases the level of protection afforded critical routers.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET OOB Timeout: IOS Procedure: The Con port should contain the following command: exec-timeout 10 0 Note: The default is 10 minutes and may not appear in the display of the configuration.

Junos Procedure: Reference the Juniper router checklist procedure guide.

###Fixes###

NET OOB Timeout: The network administrator will ensure that the timeout for unattended console port is set for no longer than 10 minutes via the exec-timeout command.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0652 CAT: 2 Modems are connected to the console or aux port

Router Type:	All Routers	Target(s):	Router
8500.2 IA Control:	ECSC-1	Category:	4.7 - Routers
Condition(s):	Router		

Vulnerability The IAO/NSO will ensure modems are not connected to the console or auxiliary ports.

Vulnerability Discussion: Access to the router via a modem is potentially very risky. If an intruder were to gain access to the router via a modem, the potential for denial of service attacks, interception of sensitive information, and other destructive actions is greatly increased.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET Modems on Mgt Ports: Physically inspect any local routers to ensure modems are not connected.

###Fixes###

NET Modems on MGT Ports: Modems are connected to routers' auxiliary or console port.

The router administrator will ensure that all modems connected to the router are disconnected. Modems should only be connected for emergency maintenance.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0655 CAT: 3 Ensure that the router's auxiliary port is disable

Router Type:	All Routers	Target(s):	Router
8500.2 IA Control:	ECSC-1	Category:	2.2 - Least Privilege
Condition(s):	Router		

Vulnerability The router administrator will ensure that the router's auxiliary port is disabled.

Vulnerability Discussion: The routers auxiliary port is typically used for remote administration via a modem. This, however, is seldom used and should therefore be disabled. Access to the router via a modem is potentially very risky. If an intruder were to gain access to the router via a modem, the potential for denial of service attacks, interception of sensitive information, and other destructive actions is greatly increased.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET Aux Port Disabled: IOS Procedure: View the router's configuration to ensure that the auxiliary port is disabled with a configuration similar to the following:

```
line aux 0
no exec
transport input none
```

Junos Procedure: Reference the Juniper router checklist procedure guide.

###Fixes###

NET Aux Ports Disabled: Auxiliary ports are not disabled on the router.

The router administrator will disable the auxiliary ports on all routers by using the following router commands:

```
line aux 0
no exec
exec-timeout 0 5
transport input none.
```

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0664 CAT: 2 Use of in-band management is not limited.

Router Type: All Routers

Target(s): Router

8500.2 IA Control: ECSC-1

Category: 4.7 - Routers

Condition(s): Router

Vulnerability The network administrator will limit the use of in-band management to situations where the use of OOB management would hinder operational commitments or when emergency situations arise. IAO/NSO will approve the use of in-band management on a case-by-case documented basis.

Vulnerability Discussion: It is imperative that communications used for administrative access to network components is limited to emergency situations or where out-of-band management would hinder daily operational requirements. In-band management introduces the risk of an attacker gaining access to the network internally or even externally.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET Inband Mgt not Limited: Interview the IAO/NSO for compliance. Ask to see documentation.

###Fixes###

NET In-band Mgt not Limited: Use out-of-band management.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0665 CAT: 1 in-band management connections require passwords

Router Type: All Routers

Target(s): Router

8500.2 IA Control: ECSC-1

Category: 1.3 - Identity Management

Condition(s): Router

Vulnerability The IAO/NSO will ensure that all in-band management connections to the router require passwords.

Vulnerability Discussion: Devices protected with weak password schemes or no password at all, provide the opportunity for anyone to crack the password or gain access to the device and cause network, device, or information damage or denial of service.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET In-band PSW Protected: IOS Procedure: Review each router's configuration to ensure that the VTY ports require a login prompt. The configuration should look similar to the following:

```
line vty 0 4
login authentication admin_only
exec-timeout 10 0
transport input ssh
```

Junos Procedure: Reference the appropriate router checklist procedure guide.

###Fixes###

NET In-band PSW Protected: The site will ensure that all in-band management connections to the router require passwords.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0667 CAT: 2 Two-factor authentication, encryption required

Router Type: All Routers

Target(s): Router

8500.2 IA Control: ECSC-1

Category: 1.1 - Passwords

Condition(s): Router

Vulnerability To ensure the proper authorized network administrator is the only one who can access the device, the IAO/NSO will ensure in-band access enforces the following security restrictions:

- Two-factor authentication (e.g., Secure ID, DOD PKI)
- Encryption of management session (FIPS 140-2 validated encryption)
- Auditing
- Two-factor authentication discussion; reference Section 3.4.3.1.

Vulnerability Discussion: Without secure management implemented with authenticated access controls, strong two-factor authentication, encryption of the management session and audit logs, unauthorized users may gain access to network managed devices compromised, large parts of the network could be incapacitated with only a few commands.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

Net Two-factor Authentication: First review the device configuration to ensure that an authentication server is being used. Then verify that a 2-factor authentication method has been implemented.

###Fixes###

NET Two-factor Authentication: The router administrator will configure the router to utilize the most currently supported version of SSH with all security patches applied. The network administrator will configure the routers to ensure authenticated access control, strong two-factor authentication, encryption of the management session and audit logs are all being incorporated in the access scheme.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0670 CAT: 2 In-band management is allowed to the routers from

Router Type:	All Routers	Target(s):	Router
8500.2 IA Control:	ECSC-1	Category:	4.7 - Routers
Condition(s):	Router		

Vulnerability The router administrator will ensure that the router only allows in-band management sessions from authorized IP addresses from the internal network.

Vulnerability Discussion: Remote administration using VTY/telnet ports is inherently dangerous because anyone with a sniffer and access to the right LAN segment, can acquire the router account and password information. With this intercepted information they could gain access to the router and cause denial of service attacks, intercept sensitive information, or perform other destructive actions.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET In-band from Auth IP Addr: Procedure: Reference the appropriate router checklist procedure guide.

###Fixes###

NET In-band Auth IP Addr: The router administrator will create an ACL for each router that restricts the use of VTY ports for remote router administration, to only authorized internal connections. The ACL configuration should look similar to the following:

```
access-list 3 permit 215.17.1.0  0.0.0.255
access-list 3 permit 215.17.34.0  0.0.0.255
access-list 3 deny any
  .
.
line vty 0 4
access-class 3 in
```

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0680 CAT: 2 FIPS 140-2 encryption required on In-band

Router Type: All Routers

Target(s): Router

8500.2 IA Control: ECSC-1

Category: 4.7 - Routers

Condition(s): Router

Vulnerability The router administrator will ensure in-band management access to the router is secured using FIPS 140-2 validated encryption such as AES, 3DES, SSH, or SSL.

Vulnerability Discussion: Remote administration using VTY/telnet ports is inherently dangerous because anyone with a sniffer and access to the right LAN segment can acquire the router account and password information. With this intercepted information they could gain access to the router and cause denial of service attacks, intercept sensitive information, or perform other destructive actions.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET FIPS 140-2 required: IOS Procedure: The configuration should look similar to the following:
line vty 0 4
transport input ssh

Junos Procedure: Reference the appropriate router checklist procedure guide.

###Fixes###

NET FIPS 140-2 required: The router administrator will ensure that only SSH connections are allowed to access VTY ports.

Display the ACLs protecting the vty ports as follows and the configuration should display something like the following:
transport input ssh. For routers that have limitations based on hardware, and can not support an IOS version that supports SSH, the transport input telnet command must be utilized.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0681 CAT: 2 Secure Shell timeout is not 60 seconds or less

Router Type: All Routers

Target(s): Router

8500.2 IA Control: ECSC-1

Category: 4.7 - Routers

Condition(s): Router

Vulnerability The router administrator will ensure SSH timeout value is set to 60 seconds or less, causing incomplete SSH connections to shut down after 60 seconds or less.

Vulnerability Discussion: Reducing the broken telnet session expiration time to 60 seconds or less strengthens the router from being attacked by use of an expired session.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

IOS Procedure: Reference the CISCO router checklist procedure guide.

JUNOS Procedure: This is NA for Juniper routers.

###Fixes###

NET SSH Timeout 60 sec: Implement Secure Shell Timeout.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0682 CAT: 2 SSH login attempts value is greater than 3

Router Type: All Routers

Target(s): Router

8500.2 IA Control: ECSC-1

Category: 4.7 - Routers

Condition(s): Router

Vulnerability The router administrator will ensure the maximum number of unsuccessful SSH login attempts is set to three, locking access to the router.

Vulnerability Discussion: Setting the authentication retry to 3 or less strengthens against a Brute Force attack.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

IOS Procedure: Reference the CISCO router checklist procedure guide.

JUNOS Procedure: This is NA for Juniper routers.

###Fixes###

NET SSH Login Attempts: Implement Secure Shell Authentication retries.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0685 CAT: 2 In-band Mgt not configured to timeout in 10 min.

Router Type: All Routers

Target(s): Router

8500.2 IA Control: ECSC-1

Category: 4.7 - Routers

Condition(s): Router

Vulnerability The router administrator will ensure the timeout for in-band management access is set for no longer than 10 minutes.

Vulnerability Discussion: Routers have multiple areas of configuration. The more critical the area, the tighter the control should be. Setting the timeout of the session to ten minutes or less increases the level of protection afforded critical routers.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET In-band Timeout 10 min: IOS Procedure: The VTY ports should contain the following command: exec-timeout 10 0Note: The default is 10 minutes and may not appear in the display of the configuration.

Junos Procedure: Reference the Juniper router checklist procedure guide.

###Fixes###

NET In-band Timeoout 10 min: The network administrator will ensure that the timeout for unattended consoles and telnet ports for no longer than 10 minutes via the exec-timeout command.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0690 CAT: 4 Logging of all in-band management access attempts

Router Type:	All Routers	Target(s):	Router
8500.2 IA Control:	ECAT-1: ECAT-2	Category:	10.2 - Content Configuration
Condition(s):	Router		

Vulnerability The router administrator will configure the ACL that is bound to the VTY ports to log permitted and denied access attempts.

Vulnerability Discussion: Audit logs are necessary to provide a trail of evidence in case the network is compromised. Without an audit trail that provides a when, where, who and how set of information, repeat offenders could continue attacks against the network indefinitely. With this information, the network administrator can devise ways to block the attack and possibly identify and prosecute the attacker.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET In-band Logging: Procedure: Reference the appropriate router checklist procedure guide.

###Fixes###

NET Inband Logging: The router administrator will add the log parameter to all access lists protecting the VTY ports. The router configuration file should display lines similar to the following:

```
access-list 3 permit tcp host x.x.x.x any eq 23 log
access-list 3 deny any log
.
line vty 0 4
access-class 3 in
```

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0700 CAT: 2 Minimum operating system release level

Router Type: All Routers

Target(s): Router

8500.2 IA Control: ECSC-1

Category: 2.2 - Least Privilege

Condition(s): Router

Vulnerability The router administrator will implement the latest stable operating system on each router IAW the current Network Infrastructure Security Checklist.

Vulnerability Discussion: Cisco IOS Software releases based on versions 11.x and 12.0 contain multiple vulnerabilities as well as being less secure. A specific defect allows a limited number of SNMP objects to be viewed and modified without authorization using an undocumented ILMI community strings.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET OS Current: IOS Procedure: Have the router administrator execute the show version command on all of the Cisco routers to verify that the installed IOS version is at 12.3 or later. Software Major Release 12.3 was posted to CCO May 19, 2003.

JUNOS Procedure: In operational mode, have the router administrator execute the show version brief command on all of the Juniper routers to verify that the installed JUNOS version is at 6.4 or later on M and T series and 5.3.2 on E series. This command will show the base OS as well as the kernel, packet forwarding engine, routing, and crypto. Validate that all software components are at the required level.

###Fixes###

NET OS Current: Later IOS Software releases contain vulnerabilities which may not have been addressed in current versions.

Operating Systems are not IAW with Network Infrastructure Security Checklist

Update Operating Systems on all routers.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0710 CAT: 3 The Cisco discovery protocol (CDP) is not disabled

Router Type: Premise Routers
Target(s): Router
8500.2 IA Control: ECSC-1
Category: 2.2 - Least Privilege
Condition(s): Router

Vulnerability The router administrator will ensure CDP is disabled on all external interfaces on Cisco premise routers.

Vulnerability Discussion: The Cisco Discovery Protocol is a proprietary protocol that CISCO routers use to identify each other on a LAN segment and is considered deleterious to security.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET CDP Internal Only: Review all Cisco router configurations to ensure that no cdp run is included in the global configuration or no cdp enable is included for each active external interface.

###Fixes###

NET CDP Internal Only: Ensure that no cdp run is included in the global configuration or no cdp enable is included for each active external interface.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0720 CAT: 3 TCP and UDP small server services are not disabled

Router Type: All Routers
Target(s): Router
8500.2 IA Control: ECSC-1
Category: 2.2 - Least Privilege
Condition(s): Router

Vulnerability The router administrator will ensure TCP & UDP small servers are disabled.

Vulnerability Discussion: TCP and UDP protocols include services (chargen, echo, etc.) that the routers can support, however, they are not required for operation. These services have been used by attackers to cause network denial of service attacks.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET TCP/UDP small -servers: IOS Procedure: Review all Cisco router configurations to verify that service udp-small-servers and service tcp-small-servers are not found.

Note: The TCP and UDP small servers are enabled by default on Cisco IOS Software Version 11.2 and earlier. They are disabled by default on Cisco IOS Software Versions 11.3 and later.

JUNOS Procedure: JUNOS does not support the echo, chargen, discard or daytime services; hence, this will never be a finding.

###Fixes###

NET TCP/UDP small-servers: The router administrator will change the router configuration files to include the following CISCO commands: no service tcp-small-servers and no service udp-small-servers, for each router running an IOS version prior to 12.0. This is the default for IOS versions 12.0 and later (I.E., these commands will not appear in the running configuration.)

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0722 CAT: 3 Service Pad is enabled on the router.

Router Type: All Routers

Target(s): Router

8500.2 IA Control: ECSC-1

Category: 4.7 - Routers

Condition(s): Router

Vulnerability The router administrator will ensure PAD services are disabled.

Vulnerability Discussion: Packet Assembler Disassembler (PAD) is a X.25 component seldom used. It collects the data transmissions from the terminals and gathers them into a X.25 data stream and vice versa. PAD acts like a multiplexer for the terminals. If enabled, it can leave your device vulnerable to attacks.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET PAD Services: IOS Procedure: Review all Cisco router configurations to verify that service pad is not found.

JUNOS Procedure: n/a

###Fixes###

NET PAD Services: The router administrator will change the router configuration files to include the following CISCO commands: no service pad

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0724 CAT: 3 TCP Keep-Alives for Telnet Session must be enabled

Router Type: All Routers

Target(s): Router

8500.2 IA Control: ECSC-1

Category: 4.7 - Routers

Condition(s): Router

Vulnerability The router administrator will ensure TCP Keep-Alives for Telnet Session are enabled.

Vulnerability Discussion: Enabling TCP keepalives on incoming connections can help guard against both malicious attacks and orphaned sessions caused by remote system crashes. Enabling the TCP keepalives causes the router to generate periodic keepalive messages, letting it detect and drop broken Telnet connections.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET TCP Keep-alives: IOS Procedure: Review all Cisco router configurations to verify that tcp-keepalives-in are enabled.

JUNOS Procedure: n/a.

###Fixes###

NET TCP Keep-alives: The router administrator will change the router configuration files to include the following CISCO commands: service tcp-keepalives in

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0726 CAT: 3 Identification support must be disabled.

Router Type: All Routers

Target(s): Router

8500.2 IA Control: ECSC-1

Category: 4.7 - Routers

Condition(s): Router

Vulnerability The router administrator will ensure identification support is disabled.

Vulnerability Discussion: Identification support allows you to query a TCP port for identification. This feature enables an unsecured protocol to report the identity of a client initiating a TCP connection and a host responding to the connection. With identification support, you can connect a TCP port on a host, issue a simple text string to request information, and receive a simple text-string reply. This is another mechanism to learn the router vendor, model number, and software version being run.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET IDENT Support disabled: Review all Cisco router configurations to verify that identification support is disabled via no identd IOS command.JUNOS Procedure: n/a.

###Fixes###

NET IDENT Support Disabled: The router administrator will change the router configuration files to include the following CISCO commands: no identd if its enabled.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0728 CAT: 3 DHCP service is not disabled on all routers.

Router Type: All Routers

Target(s): Router

8500.2 IA Control: ECSC-1

Category: 4.1 - Unneeded Ports, Protocols, and Services

Condition(s): Router

Vulnerability The router administrator will ensure DHCP Services are disabled.

Vulnerability Discussion: By sending a large packet to the Dynamic Host Configuration Protocol (DHCP) port it is possible to freeze the routers processing engine.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET DHCP disabled: IOS Procedure: Review all Cisco router configurations to verify that no service dhcp is found. Note: Service DHCP is enabled by default.

JUNOS Procedure: n/a

###Fixes###

NET DHCP Disabled: The router administrator will change the router configuration files to include the following CISCO commands: no service dhcp.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0730 CAT: 3 The finger service is not disabled on all routers.

Router Type: All Routers

Target(s): Router

8500.2 IA Control: ECSC-1

Category: 2.2 - Least Privilege

Condition(s): Router

Vulnerability The router administrator will ensure Finger is disabled.

Vulnerability Discussion: The IOS finger service supports the UNIX finger protocol, which is used for querying a host about the users that are logged on. This service is not necessary for generic users. If an attacker would find out who is using the network, they may use social engineering practices to try to elicit classified DOD information.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET Finger Disabled: IOS Procedure: Review all Cisco router configurations to verify that the IOS command, no ip finger for IOS version 12.0 and higher and no service finger for earlier version, is included.

JUNOS Procedure: Under the edit system services hierarchy, enter a show command to verify that the finger command is not present.

###Fixes###

NET Finger Disabled: The router administrator will change the router configuration files to include the CISCO command no ip finger for IOS versions 12.0 and later or no service finger command for IOS versions prior to 12.0.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0740 CAT: 2 HTTP, FTP, and BSD r-commands are not disabled

Router Type: All Routers

Target(s): Router

8500.2 IA Control: ECSC-1

Category: 2.2 - Least Privilege

Condition(s): Router

Vulnerability The router administrator will ensure HTTP, FTP, and all BSD r command servers are disabled.

Vulnerability Discussion: The additional services that the router is enabled for increases the risk for an attack since the router will listen for these services. In addition, these services provide an unsecured method for an attacker to gain access to the router.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET HTTP, FTP, and all BSD r: Procedure: Reference the appropriate router checklist procedure guide

###Fixes###

NET HTTP, FTP, and all BSD r: The router administrator will change the router configuration files to include the Cisco command, no ip http-server, for all routers with an IOS version after 11.3 and prior to 12.0. IOS versions 12.0 and later have this disabled by default and this will not appear in the running configuration.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0750 CAT: 3 The bootp service is not disabled on all routers.

Router Type:	All Routers	Target(s):	Router
8500.2 IA Control:	ECSD-1	Category:	2.2 - Least Privilege
Condition(s):	Router		

Vulnerability The router administrator will ensure Bootp server is disabled.

Vulnerability Discussion: Bootp is a user datagram protocol (UDP) that can be used by Cisco routers to access copies of Cisco IOS Software on another Cisco router running the Bootp service. In this scenario, one Cisco router acts as a Cisco IOS Software server that can download the software to other Cisco routers acting as Bootp clients. In reality, this service is rarely used and can allow an attacker to download a copy of a routers Cisco IOS Software.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET Bootp Disabled: IOS Procedure: Review all Cisco router configurations to verify that the IOS command no ip bootp server is present.

JUNOS Procedure: JUNOS does not support the bootp or any other service to automatically copy or download images of JUNOS from a server or another router; hence, this will never be a finding.

###Fixes###

NET Bootp Disabled: The router administrator will change the router configuration files to include the Cisco command, no ip bootp server, for each router.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0760 CAT: 2 Remote loading of the startup configuration is not

Router Type: All Routers

Target(s): Router

8500.2 IA Control: ECSC-1

Category: 4.7 - Routers

Condition(s): Router

Vulnerability The router administrator will ensure configuration auto-loading is disabled.

Vulnerability Discussion: The routers can find their startup configuration either in their own NVRAM or load it over the network via TFTP or Remote Copy (rcp). Obviously, loading in from the network is taking a security risk. If the startup configuration was intercepted by an attacker, it could be used to either gain access to the router.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET Boot Network: IOS Procedure: Ensure the commands boot network and service config are not included. Note: Disabled by default in version 12.0 , not be displayed in the running configuration.

JUNOS Procedure: JUNOS does not provide the ability to automatically load a configuration from another server on the network; hence, this will never be a finding.

###Fixes###

NET Boot Network: The router administrator will change the router configuration files to include the CISCO commands, no boot network and no service config, for each router.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0770 CAT: 2 IP Source Routing is not disabled on all routers.

Router Type: All Routers

Target(s): Router

8500.2 IA Control: ECSC-1

Category: 2.2 - Least Privilege

Condition(s): Router

Vulnerability The router administrator will ensure IP source routing is disabled.

Vulnerability Discussion: Source routing is a feature of IP, whereby, individual packets can specify routes. This feature is used in several different network attacks.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET Source-Route Disabled: IOS Procedure: Ensure the command no ip source-route is included.

JUNOS Procedure: Under the edit chassis hierarchy enter a show command to verify that the no-source-route command is present on all Juniper routers.

###Fixes###

NET Source-Route Disabled: The router administrator will change the router configuration files to include the CISCO command, no ip source-route, for each router.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0780 CAT: 2 The proxy ARP service is not disabled on each inte

Router Type:	All Routers	Target(s):	Router
8500.2 IA Control:	ECSC-1	Category:	2.2 - Least Privilege
Condition(s):	Router		

Vulnerability The router administrator will ensure Proxy ARP is disabled.

Vulnerability Discussion: When proxy ARP is enabled on a Cisco router, it allows that router to extend the network (at Layer 2) across multiple interfaces (LAN segments). Because proxy ARP allows hosts from different LAN segments to look like they are on the same segment, proxy ARP is only safe when used between trusted LAN segments. Attackers can leverage the trusting nature of proxy ARP by spoofing a trusted host and then intercepting packets. You should always disable proxy ARP on router interfaces that do not require it, unless the router is being used as a LAN bridge.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET IP Proxy-arp disabled: IOS Procedure: Ensure the command no ip proxy-arp is included for every active interface.

JUNOS Procedure: JUNOS does not provide the ability to extend the network at layer 2 across multiple LAN segments via proxy ARP; hence, this will never be a finding.

###Fixes###

NET IP Proxy-arp disabled: The router administrator will change the router configuration files to include the no ip proxy-arp command for each interface of every router.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0781 CAT: 2 Gratuitous ARP must be disabled.

Router Type: All Routers

Target(s): Router

8500.2 IA Control: ECSC-1

Category: 4.7 - Routers

Condition(s): Router

Vulnerability The router administrator will ensure Gratuitous ARP is disabled.

Vulnerability Discussion: A gratuitous ARP is an ARP broadcast in which the source and destination MAC addresses are the same. It is used to inform the network about a hosts IP address. A spoofed gratuitous ARP message can cause network mapping information to be stored incorrectly, causing network malfunction.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET Gratious Arp Disabled: IOS Procedure: Review all router configurations to ensure the command no ip gratuitous-arp is included for every active interface.

JUNOS Procedure: JUNOS does not provide the ability to extend the network at layer 2 across multiple LAN segments via gratuitous ARP; hence, this will never be a finding.

###Fixes###

NET Gratious Arp Disabled: The router administrator will change the router configuration files to include the no ip gratuitous-arp command for each interface of every router.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0790 CAT: 3 IP directed broadcasts are not disabled.

Router Type: All Routers

Target(s): Router

8500.2 IA Control: ECSC-1

Category: 4.7 - Routers

Condition(s): Router

Vulnerability The router administrator will ensure IP directed broadcast is disabled on all router interfaces.

Vulnerability Discussion: An IP directed broadcast is a datagram sent to the broadcast address of a subnet that is not directly attached to the sending machine. The directed broadcast is routed through the network as a unicast packet until it arrives at the target subnet, where it is converted into a link-layer broadcast. Because of the nature of the IP addressing architecture, only the last router in the chain, which is connected directly to the target subnet, can conclusively identify a directed broadcast.

IP directed broadcasts are used in the extremely common and popular smurf, or Denial of Service (DoS), attacks. In a smurf attack, the attacker sends ICMP echo requests from a falsified source address to a directed broadcast address, causing all the hosts on the target subnet to send replies to the falsified source. By sending a continuous stream of such requests, the attacker can create a much larger stream of replies, which can completely inundate the host whose address is being falsified. This service should be disabled on all interfaces when not needed to prevent smurf and DoS attacks.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET Direct Broadcast: IOS Procedure: IP directed broadcast is disabled by default in IOS version 12.0 and higher so the command no ip directed-broadcast will not be displayed in the running configuration—verify that the running configuration does not contain the command ip directed-broadcast. For versions prior to 12.0 ensure the command no ip directed-broadcast is displayed in the running configuration.

JUNOS Procedure: JUNOS does not forward directed broadcasts; hence, this will never be a finding.

###Fixes###

NET Direct Broadcast: The router administrator will change the router configuration files to disable the IP directed broadcast on all interfaces.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0800 CAT: 2 ICMP unreachable notifications, mask replies, and

Router Type: Premise Routers

Target(s): Router

8500.2 IA Control: ECSC-1

Category: 4.7 - Routers

Condition(s): Router

Vulnerability The router administrator will ensure ICMP unreachable notifications, mask replies, and redirects are disabled on all external interfaces of the premise router.

Vulnerability Discussion: The Internet Control Message Protocol (ICMP) supports IP traffic by relaying information about paths, routes, and network conditions. Routers automatically send ICMP messages under a wide variety of conditions. Three ICMP messages are commonly used by attackers for network mapping and diagnosis: Host unreachable, Redirect, and Mask Reply.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET ICMP Unreachables: Procedure: Reference the appropriate router checklist procedure guide.

###Fixes###

NET ICMP Unreachables: The router administrator will change the router configuration files to include the Cisco commands no ip unreachables and no ip redirects. The IOS command no ip mask-reply is disabled by default and will not appear in the running configuration.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0810 CAT: 3 Two NTP servers have not been specified to the rou

Router Type: Premise Routers

Target(s): Router

8500.2 IA Control: ECSC-1

Category: 4.7 - Routers

Condition(s): Router

Vulnerability The IAO/NSO will ensure that two Network Time Protocol (NTP) servers are defined on the premise router to synchronize its time.

Vulnerability Discussion: Without synchronized time, accurately correlating information between devices becomes difficult, if not impossible. When it comes to security, if you cannot successfully compare logs between each of your routers, you will find it very hard to develop a reliable picture of an incident.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET NTP - Two required: Reference the appropriate router checklist procedure guide.

###Fixes###

NET NTP Two requireed: Specify two NTP server IP addresses on the routers to prevent NTP messages from being received from non-authorized sources.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0811 CAT: 2 Network Time Protocol (NTP) servers must be define

Router Type: All Routers
Target(s): Router
8500.2 IA Control: ECSC-1
Category: 4.7 - Routers
Condition(s): Router

Vulnerability The IAO/NSO will ensure that the premise router is acting as an NTP server for only internal clients.

Vulnerability Discussion: The NTP time-servers can not provide services for external clients due to the high vulnerability.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET NTP Internal Clients Only: Procedure: If NTP Servers are defined, review the router configurations and verify that NTP servers have been defined for internal clients.

###Fixes###

NET NTP Internal Clients Only: Install the server to service internal clients only.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0812 CAT: 1 NTP clients receiving services from external NTP s

Router Type: All Routers
Target(s): Router
8500.2 IA Control: ECSC-1
Category: 4.7 - Routers
Condition(s): Router

Vulnerability The IAO/NSO will ensure that all internal routers are configured to use the premise router to synchronize time.

Vulnerability Discussion: NTP is insecure and without peering within the enclave Network Time Protocol can be used by an attacker to send NTP packets to crash or overload the router.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET NTP Client use Premise: IOS Procedure: Review the router configurations and verify that NTP clients have been defined similar to the following example:
ntp server 129.237.32.2 (source IP address of server)

JUNOS Procedure: Review the router configurations and verify that NTP servers have been defined similar to the following example:
[edit system]
ntp {
boot-server 129.237.32.2;
server 129.237.32.2;
server 142.181.31.6;
}

###Fixes###

NET NTP Client use Premise: Implement a secure NTP process using a local NTP server.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0820 CAT: 3 Premise router is configured as a client revolver

Router Type: Premise Routers

Target(s): Router

8500.2 IA Control: ECSC-1

Category: 4.7 - Routers

Condition(s): Router

Vulnerability The IAO/NSO will ensure that the DNS servers are defined if the router is configured as a client resolver.

Vulnerability Discussion: The susceptibility of IP addresses to spoofing translates to DNS host name and IP address mapping vulnerabilities. For example, suppose a source host wishes to establish a Telnet connection with a destination host and queries a DNS server for the IP address of the destination host name. If the response to this query is the IP address of a host operated by an attacker, the source host will establish a connection with the attackers host, rather than the intended target. The user on the source host might then provide logon, authentication, and other sensitive data.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET DNS Servers for Client: Reference the appropriate router checklist procedure guide.

###Fixes###

NET DNS Servers for Clients: The router administrator will change the router configuration files to include the primary and secondary domain servers by adding the Cisco command, ip name-server x.x.x.x x.x.x.x, for each router. Note: fill in the IP addresses after the ip name-server command with the correct primary and secondary name server addresses for the network.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0890 CAT: 2 SNMP access is not restricted to approved IP addre

Router Type: All Routers

Target(s): Router

8500.2 IA Control: ECSC-1

Category: 4.7 - Routers

Condition(s): Router

Vulnerability The router administrator will restrict SNMP access to the router from only authorized internal IP addresses.

Vulnerability Discussion: Detailed information about the network is sent across the network via SNMP. If this information is discovered by attackers it could be used to trace the network, show the networks topology, and possibly gain access to network devices.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET SNMP Access Restricted: Reference the appropriate router checklist procedure guide.

###Fixes###

NET SNMP Access Restricted: The router administrator will change the router configuration files to include ACLs to limit access to SNMP sessions to allowed IP addresses only. The configuration should be similar to the following: access-list XX permit host x.x.x.x; snmp-server community clear text string ro XX

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0892 CAT: 2 SNMP access is not restricted to the internal netw

Router Type: All Routers

Target(s): Router

8500.2 IA Control: ECSC-1

Category: 4.7 - Routers

Condition(s): Router

Vulnerability The router administrator will ensure SNMP is blocked at all external interfaces.

Vulnerability Discussion: Detailed information about the network is sent across the network via SNMP. If this information is discovered attackers, it could be used to trace the network, show the networks topology, and gain access to network devices.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET SNMP External IP Blocked: Verify that the IP addresses permitted SNMP access to the routers belong to the internal network.

###Fixes###

NET SNMP External IP Blocked: The router administrator will change the router configuration files to include to limit access to SNMP sessions to the internal network.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0894 CAT: 2 SNMP write access to the router is enabled.

Router Type: All Routers

Target(s): Router

8500.2 IA Control: ECSC-1

Category: 4.7 - Routers

Condition(s): Router

Vulnerability The router administrator will ensure SNMP is only enabled in the read mode; Read/Write is not enabled unless approved and documented by the IAO/NSO.

Vulnerability Discussion: Enabling write access to the router via SNMP provides a mechanism that can be exploited by an attacker to set configuration variables that can disrupt network operations.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET SNMP Read/Write Access: Reference the appropriate router checklist procedure guide.

###Fixes###

NET SNMP Read/Write Access: Disable SNMP write access to the router.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0910 CAT: 2 Router is not compliant with DOD Instr. 8551.1

Router Type: Premise Routers

Target(s): Router

8500.2 IA Control: ECSC-1

Category: 2.2 - Least Privilege

Condition(s): Router

Vulnerability The router administrator will utilize ingress and egress ACLs to restrict traffic in accordance with the guidelines contained in DOD Instruction 8551.1 for all ports and protocols required for operational commitments.

Vulnerability Discussion: Access Control Lists (ACLs) are the first line of defense in a layered security approach. They permit authorized packets and deny unauthorized packets based on port or service type. They enhance the posture of the network by not allowing packets to even reach a potential target within the security domain. The list provided are highly susceptible ports and services that should be blocked or limited as much as possible without adversely affecting customer requirements. Auditing packets attempting to penetrate the network but are stopped by an ACL will allow network administrators to broaden their protective ring and more tightly define the scope of operation.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET 8551.1 Ports & Protocols: Procedure: Review the running or active configuration of the premise router and verify that the router's filters are IAW DoD Ports Protocols Services Category Assignment List (PPS CAL) http://iase.disa.mil/ports/index.html.

###Fixes###

NET 8551.1 Ports & Protocols: The router administrator will utilize ingress and egress ACLs to restrict traffic in accordance with the guidelines contained in DOD Instruction 8551.1 for all services and protocols required for operational commitments.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0920 CAT: 2 The ingress and egress filters are not applied to

Router Type: Premise Routers

Target(s): Router

8500.2 IA Control: ECSC-1

Category: 4.7 - Routers

Condition(s): Router

Vulnerability The router administrator will bind the ingress ACL filtering packets entering the network to the external interface, and bind the egress ACL filtering packets leaving the network to the internal interface—both on an inbound direction.

Note: All filters must be applied to the appropriate interfaces on an inbound direction. Ingress filtering is applied to all traffic entering the enclave. The ingress filter would be bound to all external interfaces. Since egress filtering is applied to all traffic leaving the enclave, this filter would be bound to all internal interfaces.

Vulnerability Discussion: If illegal packets are not dropped immediately at the proper interface, the routing engine could be come constrained or consume router resources trying to route packets to the next interface; thereby potentially creating a DoS situation.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET ACLs Bound to Interface: Reference the appropriate router checklist procedure guide.

###Fixes###

NET ACLs Bound to Interface: Bind the ingress ACL to the external interface (inbound) and the egress ACL to the internal interface (inbound).

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0940 CAT: 1 Ingress Filtering Inbound Spoofing Addresses

Router Type: Premise Routers

Target(s): Router

8500.2 IA Control: ECSC-1

Category: 4.7 - Routers

Condition(s): Router

Vulnerability The router administrator will restrict the premise router from accepting any inbound IP packets with a source address that contain an IP address from the internal network, any local host loop back address (127.0.0.0/8), the link-local IP address range (169.254.0.0/16), IANA unallocated addresses or any reserved private addresses in the source field.

Vulnerability Discussion: Inbound spoofing occurs when someone outside the network uses an internal IP address to gain access to systems or devices on the internal network. If the intruder is successful, they can intercept data, passwords, etc., and use that information to perform destructive acts on or to the network.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET Ingress Spoofing Filter: Reference the appropriate router checklist procedure guide.

###Fixes###

NET Ingress Spoofing Filter: The router administrator will configure the router ACLs to restrict inbound IP addresses that contain any IP addresses from the internal network, local host addresses, link-local DHCP default address (169.254.0.0) or any reserved private addresses as documented in RFC 1918 in the source field. The following can be used as a model:

```
interface eth0/0
description external int
ip address interface IP address  subnet mask
ip access-group 100 in


access-list 100 deny ip internal network ip range   wildcard mask any log
access-list 100 deny ip 127.0.0.0 0.255.255.255 any log
access -list 100 deny ip 10.0.0.0 0.255.255.255 any log
access-list 100 deny ip 172.16.0.0 0.15.255.255 any log
access-list 100 deny ip 192.168.0.0 0.0.255.255 any log
access-list 100 deny ip 169.254.0.0 0.0.255.255 any log
```

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0950 CAT: 1 Egress Outbound Spoofing Filter

Router Type: Premise Routers

Target(s): Router

8500.2 IA Control: ECSC-1

Category: 4.7 - Routers

Condition(s): Router

Vulnerability The router administrator will restrict the router from accepting any outbound IP packet that contains an illegitimate address in the source address field via egress ACL or by enabling Unicast Reverse Path Forwarding.

Vulnerability Discussion: Access Control Lists (ACLs) are the first line of defense in a layered security approach. They permit authorized packets and deny unauthorized packets based on port or service type. They enhance the posture of the network by not allowing packets to even reach a potential target within the security domain. The list provided are highly susceptible ports and services that should be blocked or limited as much as possible without adversely affecting customer requirements. Auditing packets attempting to penetrate the network but are stopped by an ACL will allow network administrators to broaden their protective ring and more tightly define the scope of operation.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET Egress Spoofing Filter: Reference the appropriate router checklist procedure guide.

###Fixes###

NET Egress Spoofing Filter: The NSO will ensure that an ACL is configured to restrict the router from accepting any outbound IP packet that contains an external IP address in the source field.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0960 CAT: 2 Routers are not set to intercept TCP SYN attacks f

Router Type:	Premise Routers	Target(s):	Router
8500.2 IA Control:	ECSC-1	Category:	2.2 - Least Privilege
Condition(s):	Router		

Vulnerability The IAO/NSO will implement features provided by the router to protect servers from any TCP SYN flood attacks from an outside network.

Vulnerability Discussion: The TCP SYN attack involves transmitting a volume of connections that cannot be completed at the destination. This attack causes the connection queues to fill up, thereby denying service to legitimate TCP users.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET TCP SYN Protection: Procedure: Reference the appropriate router checklist procedure guide.

CAVEAT: If the site has implemented SYN flood protection for the network using the perimeter firewall, there is not an additional requirement to implement it on the router.

###Fixes###

NET TCP SYN Protection: The NSO will ensure that the TCP Intercept command is used to intercept TCP SYN attacks from outside the network.

The ACL configuration should be similar to the following:

ip tcp intercept list 107;
access-list 107 permit tcp any internal network wildcard mask

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0965 CAT: 2 Routers are not configured to protect themselves a

Router Type: All Routers

Target(s): Router

8500.2 IA Control: ECSC-1

Category: 2.2 - Least Privilege

Condition(s): Router

Vulnerability The router administrator will set the maximum wait interval for establishing a TCP connection request to the router to 10 seconds or less, or implement a feature to rate-limit TCP SYN traffic destined to the router.

Vulnerability Discussion: The TCP SYN attack involves transmitting a volume of connections that cannot be completed at the destination. This attack causes the router connection queues to fill up, thereby denying service to router administrators or BGP peers.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET TCP synwait-time 10: IOS Procedure: Review the premise or edge router configuration to ensure the ip tcp synwait-time command is in place to monitor TCP connection requests to the router. The configuration should look similar to the following: ip tcp synwait-time 10

JUNOS Procedure: Reference the appropriate router checklist procedure guide.

###Fixes###

NET TCP synwait-time 10: The IAO will ensure that the ip tcp synwait-time has been configured on Cisco routers or rate limiting of TCP SYN traffic on Juniper routers.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0966 CAT: 2 Routers are not configured with CEF enabled to pro

Router Type: All Routers

Target(s): Router

8500.2 IA Control: ECSC-1

Category: 2.2 - Least Privilege

Condition(s): Router

Vulnerability The router administrator will enable CEF to improve router stability during a SYN flood attack to the network.

Vulnerability Discussion: The Cisco Express Forwarding (CEF) switching mode replaces the traditional Cisco routing cache with a data structure that mirrors the entire system routing table. Because there is no need to build cache entries when traffic starts arriving for new destinations, CEF behaves more predictably when presented with large volumes of traffic addressed to many destinationssuch as a SYN flood attacks that. Because many SYN flood attacks use randomized source addresses to which the hosts under attack will reply to, there can be a substantial amount of traffic for a large number of destinations that the router will have to handle. Consequently, routers configured for CEF will perform better under SYN floods directed at hosts inside the network than routers using the traditional cache.

Note: Junipers FPC (Flexible PIC Concentrator) architecture with the integrated Packet Forwarding Engine provides similar functionality and capabilities and is far superioer than the traditonal routing cache that is vulnerable to a DoS attack described above. The forwarding plane on all Juniper M and T Series platforms are built around this architecture and therefore is not configurable.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET CEF enabled: IOS Procedure: Review all Cisco routers to ensure that CEF has been enabled. The configuration should like similar to the following: ip cef

JUNOS Procedure: The forwarding plane on all Juniper M and T Series platforms are built around the FPC (Flexible PIC Concentrator) architecture that has similar capabilities as CEF. FPC is not configurable and is totally integrated with the Packet Forwarding Engine; hence, this will always be not a finding.

CAVEAT: If the site has implemented SYN flood protection for the network using the perimeter firewall, there is not an additional requirement to implement it on the router.

###Fixes###

NET CEF enabled: The IAO will ensure that the ip cef command has been configured on Cisco routers.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0980 CAT: 2 Routers are not configured to block inbound exploi

Router Type: Premise Routers

Target(s): Router

8500.2 IA Control: ECSC-1

Category: 2.2 - Least Privilege

Condition(s): Router

Vulnerability The router administrator will block all inbound ICMP messages with the exception of Echo Reply (type 0), and Time Exceeded (type 11). ICMP message number 3, code 4, are permitted inbound with the following exception: Must be denied from external AG addresses, otherwise permitted.

Vulnerability Discussion: Using inbound ICMP Echo, Information, Net Mask, and Timestamp Requests, an attacker can create a map of the subnets and hosts behind the router. An attacker can perform a denial of service attack by flooding the router or internal hosts with Echo packets. With inbound ICMP Redirect packets, the attacker can change a hosts routing tables.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET ICMP Ingress Filter: Reference the appropriate router checklist procedure guide.

###Fixes###

NET ICMP Ingress Filter: The router administrator will configure the router to include controls to block inbound exploitable ICMP traffic message types. The configuration should look similar to the following:

```
access-list 100 permit icmp any any echo-reply
access-list 100 permit icmp any any time-exceeded
access-list 100 permit icmp any any unreachable
access-list 100 deny icmp any any log
```

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET0990 CAT: 2 Routers are not configured to block all outbound I

Router Type: Premise Routers

Target(s): Router

8500.2 IA Control: ECSC-1

Category: 2.2 - Least Privilege

Condition(s): Router

Vulnerability The router administrator will block outbound ICMP traffic message types except Echo Request (type 8), Parameter Problem (type 12), and Source Quench (type 4) Destination Unreachable - Fragmentation Needed and Don't Fragment was Set (type3, code 4).

Vulnerability Discussion: An attacker from the internal network (behind the router) may be able to launch denial of service attacks with outbound ICMP packets. It is important to block all unnecessary ICMP traffic message types.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET ICMP Egress Filter: Reference the appropriate router checklist procedure guide.

###Fixes###

NET ICMP Egress Filter: The router administrator will configure the router to include controls to block outbound ICMP traffic message types except Echo, Parameter Problem and Source Quench. The configuration should look similar to the following:

access-list 107 permit icmp internal network wildcard mask any echo
access-list 107 permit icmp internal network wildcard mask any parameter-problem
access-list 107 permit icmp internal network wildcard mask any source-quench
access-list 107 permit icmp internal network wildcard mask any packet-too-big
access-list 107 deny icmp any any log

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1000 CAT: 3 Routers are not configured to block all inbound tr

Router Type: Premise Routers

Target(s): Router

8500.2 IA Control: ECSC-1

Category: 2.2 - Least Privilege

Condition(s): Router

Vulnerability The router administrator will block all inbound traceroutes to prevent network discovery by unauthorized users.

Vulnerability Discussion: An attacker can use traceroute responses to create a map of the subnets and hosts behind the router. This data may be used to mount attacks on these network subnets and hosts.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET Traceroutes blocked: Procedure: Reference the appropriate router checklist procedure guide

###Fixes###

NET Traceroutes blocked: The router administrator will configure the router to include controls to block inbound traceroutes. The configuration should look similar to the following:

access-list 100 deny icmp any any traceroute log
access-list 100 deny udp any any range 33400 34400 log

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1010 CAT: 1 Router is not configured to block known DDoS ports

Router Type: Premise Routers

Target(s): Router

8500.2 IA Control: DCBP-1: DCPP-1: ECSC-1

Category: 2.2 - Least Privilege

Condition(s): Router

Vulnerability The router administrator will block known DDoS attack ports in accordance with DOD Instruction 8551.1, Required Filtering Rules.

Vulnerability Discussion: Several high-profile Distributed Denial of Service (DDoS) attacks have been observed on the Internet. While routers cannot prevent DDoS attacks in general, it is usually sound security practice to discourage the activities of specific DDoS agents (a.k.a. zombies) by adding access list rules that block their particular ports.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET Block known DDoS: Procedure: Ensure the following are incorporated into the premise router's ingress and egress filters:

27665 31335 27444	TRINOO DDoS systems
31337 31338	Back Orifice system
16660 65000	Stacheldraht DDoS system
33270 39168	TrinityV3 system
47017	T0rn rootkit system
6711 6712 6776 6669 2222 7000	Subseven DDoS system and some variants
2001	Der Spaeher, Trojan Cow
65301	PCAnywhere

###Fixes###

NET Block known DDoS : The router administrator will configure router ACLs to prevent known DDoS attacks. Configurations for each blocking ACL should be as follows:

TRINOO DDoS:
access-list 170 deny tcp any any eq 27665 log;
access-list 170 deny udp any any eq 31335 log;
access-list 170 deny udp any any eq 27444 log;
Back Orifice DDoS:
access-list 170 deny udp any any eq 31337 log;
Stacheldraht DDoS:
access-list 170 deny tcp any any eq 16660 log;
access-list 170 deny tcp any any eq 65000 log;
TrinityV3 DDoS:
access-list 170 deny tcp any any eq 33270 log;
access-list 170 deny tcp any any eq 39168 log;
T0rn rootkit DDoS:
access-list 170 deny tcp any any eq 47017 log;
Subseven DDoS system and some variants:
access-list 170 deny tcp any any range 6711 6712 log;
access-list 170 deny tcp any any eq 6776 log;
access-list 170 deny tcp any any eq 6669 log;
access-list 170 deny tcp any any eq 2222 log;
access-list 170 deny tcp any any eq 7000 log;

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1020 CAT: 3 A log or syslog statement does not follow all deny

Router Type: Premise Routers

Target(s): Router

8500.2 IA Control: ECAT-1: ECAT-2: ECSC-1

Category: 10.2 - Content Configuration

Condition(s): Router

Vulnerability The router administrator will ensure that all attempts to any port, protocol, or service that is denied are logged.

Vulnerability Discussion: Auditing and logging are key components of any security architecture. It is essential security personnel know what is being done, attempted to be done, and by whom in order to compile an accurate risk assessment. Auditing the actions on routers provides a means to recreate an attack, or simply identify a misconfigured configuration.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET Log Denied PPS denied: Reference the appropriate router checklist procedure guide.

###Fixes###

NET Log Denied PPS denied: The IAO will ensure that all deny statements in the ACL of the router have a log statement that follows. For example:

access-list 170 deny tcp any any eq 6669 log.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1021 CAT: 3 Router must log severity levels.

Router Type: All Routers

Target(s): Router

8500.2 IA Control: ECAT-1: ECAT-2: ECSC-1

Category: 10.2 - Content Configuration

Condition(s): Router

Vulnerability The router administrator will configure all routers to log severity levels 0 through 6 and send log data to a syslog server.

Vulnerability Discussion: Logging is a critical part of router security. Maintaining an audit trail of system activity logs (syslog) can help identify configuration errors, understand past intrusions, troubleshoot service disruptions, and react to probes and scans of the network. Syslog levels 0-6 are the levels required to collect the necessary information to help in the recovery process.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET Log Severity Levels: Reference the appropriate router checklist procedure guide.

###Fixes###

NET Log Severity Levels: The router administrator will configure the router to log message severity levels 0-6 and send syslog messages to the syslog server.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1025 CAT: 3 A centralized syslog server has not been deployed.

Router Type:

Target(s): Syslog Server

8500.2 IA Control: ECTB-1: ECSC-1: ECTB-1: ECTB-1: ECSC-1: ECTB-1

Category: 10.5 - Retention

Condition(s): Syslog Server: Syslog Server

Vulnerability The IAO/NSO will ensure a centralized syslog server is deployed and configured by the syslog administrator to store all syslog messages for a minimum of 30 days online and then stored offline for one year.

Vulnerability Discussion: Logging is a critical part of router security. Maintaining an audit trail of system activity logs (syslog) can help identify configuration errors, understand past intrusions, troubleshoot service disruptions, and react to probes and scans of the network.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET Syslog SRV Log Retention: Examine the syslog server to verify that it is configured to store messages for at least 30 days. Have the administrator show you the syslog files stored offline for one year.

###Fixes###

NET Syslog SRV Log Retention: The router administrator will configure the syslog server to store messages for at least 30 days on-line. The router administrator will establish a syslog storage strategy for storing the logs off-line for minimum of 1 year.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1027 CAT: 3 The syslog server is not configured to collect sys

Router Type:

Target(s): Syslog Server

8500.2 IA Control: ECAT-1: ECAT-2: ECAT-1: ECAT-2: ECSC-1: ECAT-1: ECAT-2: ECAT-1: ECAT-2: ECSC-1

Category: 10.2 - Content Configuration

Condition(s): Syslog Server: Syslog Server

Vulnerability The syslog administrator will configure the syslog sever to collect syslog messages from levels 0 through 6.

Vulnerability Discussion: Logging is a critical part of router security. Maintaining an audit trail of system activity logs (syslog) can help identify configuration errors, understand past intrusions, troubleshoot service disruptions, and react to probes and scans of the network. Syslog levels 0-6 are the levels required to collect the necessary information to help in the recovery process.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET Syslog Srv Severity Codes: Review the syslog server configuration to ensure that it is collecting syslog messages levels 0 through 6 for the appropriate facilities (Cisco routers default to Local7).

###Fixes###

NET Syslog Srv Severity Codes: The router administrator will configure the router and syslog server to collect syslog messages levels 0 through 6.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1150 CAT: 3 Restrict messages to the Syslog Server.

Router Type:

Target(s): Syslog Server

8500.2 IA Control: ECSC-1

Category: 2.1 - Object Permissions

Condition(s): Syslog Server

Vulnerability The syslog administrator will configure the syslog server to accept messages only from authorized devices (restricting access via source and destination IP address).

Vulnerability Discussion: Restrict access to the Syslog server by approved IP addresses/users. If an unauthorized user gains access to the Syslog server and it is compromised, access to critical network information would be available. This information could be used to mount attacks against the network.

References:

Checks/Fixes:

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1030 CAT: 3 The running and startup router configurations are

Router Type: All Routers

Target(s): Router

8500.2 IA Control: COBR-1: ECSC-1

Category: 4.7 - Routers

Condition(s): Router

Vulnerability The router administrator, when saving and loading configurations will ensure that the running and startup configurations are synchronized.

Vulnerability Discussion: If the running and startup router configurations are not synchronized properly and a router malfunctions, it will not restart with all of the recent changes incorporated. If the recent changes were security related, then the routers would be vulnerable to attack.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET Start & Run CFGs in Sync: IOS Procedure: With online editing, the show running-config command will only show the current running configuration settings, which are different from the IOS defaults. The show startup-config command will show the NVRAM startup configuration. Compare the two configurations to ensure they are synchronized.

JUNOS Procedure: This will never be a finding. The active configuration is stored on flash as juniper.conf. A candidate configuration allows you to make configuration changes while in configuration mode without initiating operational changes. The router implements the candidate configuration when it is committed; thereby, making it the new active configuration—at which time it will be stored on flash as juniper.conf and the old juniper.conf will become juniper.conf .1.

###Fixes###

Start & Run CFGs in Sync: The router administrator will ensure that all router running and startup configurations are synchronized. As part of the router configuration SOP, add procedures to keep these two configurations synchronized.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1040 CAT: 4 The current and previous router configurations are

Router Type:	All Routers	Target(s):	Router
8500.2 IA Control:	COBR-1: ECSC-1	Category:	4.7 - Routers
Condition(s):	Router		

Vulnerability The router administrator will ensure at least the current and previous router configurations are stored in a secured location to ensure a proper recovery path.

Vulnerability Discussion: If the router, as well as, volatile and non-volatile memory are lost without a recent configuration stored in an offline location, it may take time to recover that segment of the network. Subscribers connected directly to that router may be without service for a longer than acceptable time.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET Backup Configurations: IOS Procedure: Have the router administrator show you the stored configuration files. At a minimum, a copy of the current and previous router configurations must be saved.

JUNOS Procedure: With Juniper, this is built in and would never be a finding. Previously committed configurations 0 – 4 are saved on flash and configurations 5 – 9 are saved on the router's hard drive. Any one of these can be used for recovery via a rollback command.

###Fixes###

NET Backup Configurations: The router administrator will store the current and previous router configurations in a secure location.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1050 CAT: 3 Access to stored configuration files is not restri

Router Type: All Routers

Target(s): Router

8500.2 IA Control: COBR-1: ECSC-1

Category: 2.2 - Least Privilege

Condition(s): Router

Vulnerability The IAO/NSO will ensure that on the system where the configuration files are stored, the router administrator uses the local operating system's security mechanisms for restricting access to the files (i.e., password restricted file access).

The IAO/NSO will ensure only authorized router administrators are given access to the stored configuration files.

Vulnerability Discussion: Many attacks on DOD computer systems are launched from within the network by unsatisfied or disgruntled employees, therefore, it is imperative that router configurations are stored in a secure location where only authorized users can gain access. If the router network is compromised, then large parts of the network could be incapacitated with only a few commands.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET BU CFG Security: Have the router administrator display the security features that are used to control access to the configuration files.

#########

NET BUs for Auth Users: Interview the IAO/NSO to ensure that access to stored configuration files is restricted to authorized router administrators only. Password restricted access to these files will be enforced and the passwords will be changed when authorized administrators leave or change job responsibilities.

###Fixes###

NET BU CFG Security: The router administrator will store the current and previous router configurations in a secure area (file access permissions restricting to authorized personnel).

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1060 CAT: 1 Unencrypted passwords are stored in plain text in

Router Type: All Routers

Target(s): Router

8500.2 IA Control: ECSC-1

Category: 1.6 - Documentation and Storage

Condition(s): Router

Vulnerability The router administrator will not store unencrypted router passwords in an offline configuration file.

Vulnerability Discussion: Many attacks on DOD computer systems are launched from within the network by unsatisfied or disgruntled employees, therefore, it is imperative that all router passwords are encrypted so they cannot be intercepted by viewing the console. If the router network is compromised, then large parts of the network could be incapacitated with only a few commands.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET Password Storage: Review the stored router configuration files to ensure passwords are not stored in plain-text format.

###Fixes###

NET Password Storage: The router administrator will ensure that any router passwords that are stored, are encrypted. Delete any un-encrypted passwords that are currently stored as part of a router configuration file. Incorporate the storage of encrypted passwords as part of the router SOP.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1070 CAT: 2 TFTP used without written approval.

Router Type: All Routers

Target(s): Router

8500.2 IA Control: DCBP-1: ECSC-1

Category: 12.9 - Documentation

Condition(s): Router

Vulnerability The IAO/NSO will authorize and maintain justification for all TFTP implementations.

Vulnerability Discussion: TFTP requies no password.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET TFTP Authorization: Verify written authorization is with the IAO. Review and recommend the procedures defined in the procedures guide.

###Fixes###

NET TFTP Authorization: The router administrator will ensure that FTP is used to transfer router configuration files to and from the router if TFTP has not been authorized by the IAO.. Change the routers configuration to include FTP setup information as follows: Address or name of remote host [?] x.x.x.x; Source file name [?] path/filename; Destination filename [?] path/filename.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1071 CAT: 2 TFTP server access is not restricted.

Router Type: All Routers

Target(s): Router

8500.2 IA Control: ECSC-1

Category: 4.7 - Routers

Condition(s): Router

Vulnerability If TFTP implementation is used, the router administrator will ensure the TFTP server resides on a controlled managed LAN subnet, and access is restricted to authorized devices within the local enclave.

Vulnerability Discussion: TFTP requires restricted and limited access.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET TFTP Server on Secure LAN: Identify TFTP server addresses and determine if LAN has traffic restrictions and devices with access to servers have ACL permissions and restrictions.

###Fixes###

TFTP Server on Secure LAN: Identify host addresses that will access the TFTP server and harden access to the server via ACL rules.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1080 CAT: 2 The FTP username and password are not configured.

Router Type: All Routers

Target(s): Router

8500.2 IA Control: ECSC-1: IAIA-1: IAIA-2

Category: 1.3 - Identity Management

Condition(s): Router

Vulnerability The router administrator will ensure the FTP username and password are configured.

Vulnerability Discussion: Transferring IOS configuration files without using the FTP service may leave the router accounts and passwords unencrypted during the transfer. If this information is intercepted during the transfer, the router could be compromised and large parts of the network could be incapacitated with only a few commands.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

IOS Procedure: IOS Procedure: Review the running config for all routers to ensure a username and password have been configured for the router's ftp client. The configuration should look similar to the following:

ip ftp username userid
ip ftp password psw.

JUNOS Procedure: not applicable.

###Fixes###

IOS Procedure: The router administrator will change the router configuration files to ensure the IP FTP command is being used to include the FTP username and password. To enable IP FTP in IOS:

ip ftp username user;
ip ftp password string;
ip ftp source-interface ether x

JUNOS: not applicable.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1110 CAT: 2 Configuration changes and service parameters are n

Router Type: All Routers

Target(s): Router

8500.2 IA Control: DCCB-1: DCCB-2: ECSC-1

Category: 12.4 - CM Process

Condition(s): Router

Vulnerability

IAO/NSO will ensure all router changes and updates are documented in a manner suitable for review.

The IAO/NSO will ensure request forms are used to aid in recording the audit trail of router change request.

The IAO/NSO will ensure changes and modifications to routers are audited so that they can be reviewed.

The router administrator will ensure current paper or electronic copies of router configurations are maintained in a secure location.

The IAO/NSO will ensure only authorized personnel, with proper verifiable credentials, are allowed to request changes to routing tables or service parameters.

Vulnerability Discussion: Router configurations are tedious to create, especially in the midst of a crisis or recovering from failure. Having stored copies of the configuration leads to quick recovery and maintains standardization from pre-failure to post-failure operations. Limiting the number of people that can change router tables and service parameters limits the chance of errors and thus limits the chance of creating a denial-of-service vulnerability. Using a form to record requests to configuration changes ensures continuity between security personnel and operations personnel. It also enhances the audit trail and checks and balances.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET CM Process not Controlled: Have the IAO/NSO provide copies of router change request forms for visual inspection.

Have the IAO/NSO provide copies of router change request forms for visual inspection.

Interview IAO/NSO and router administrator to verify compliance.

###Fixes###

CM Process not Controlled: Record router configuration changes and review periodically.

Limit changes to routing tables or service parameters to authorized personnel only.

Develop and use a form or tracking mechanism to aid in the audit trail of any router changes requested of the NSO.

Store current router configurations in a secure location.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1160 CAT: 2 Firewall implemeted and configured properly.

Router Type:

Target(s): Firewall - Data Network

8500.2 IA Control: EBBD-1: EBBD-2: EBBD-3: ECSC-1

Category: 4.3 - Firewall

Condition(s): Firewall - Data Network

Vulnerability The IAM will ensure that a firewall has been implemented to protect the entire facility and has been configured with a deny-by-default policy.

Vulnerability Discussion: Not having a filtering device enforcing the most restrictive policy possible could allow for paths the hackers can exploit in the perimeter defenses. For the purpose of this check, if the site has a packet-filtering device (firewall or router), stateful-inspection firewall, or application level firewall they meet the intent as long as the device is in a deny by default posture and what is allowed thru the device is in compliance with Appendix G of the Network Infrastructure STIG.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

Firewall Perimeter Protection: Review network topology diagram and physical connections to the firewall.

Review the firewall rules and filters to validate deny-by-default policy.

###Fixes###

Firewall Perimeter Protection: Have the NSO incorporate the Deny-by-default posture into the network perimeter defenses.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1162 CAT: 2 Firewall policy is not IAW 8551.1 & Appendix C.

Router Type:

Target(s): Firewall - Data Network

8500.2 IA Control: DCPP-1: ECSC-1

Category: 4.3 - Firewall

Condition(s): Firewall - Data Network

Vulnerability The IAM will ensure that the firewall policy is in accordance with DOD Instruction 8551.1. http://www.dtic.mil/whs/directives/corres/html/85511.htm and Appendix C of this document.

Vulnerability Discussion: After the premise router, the firewall is the next line of defense in a layered security approach. The rules and filters should only permit authorized packets and deny unauthorized packets based on port or service type for both inbound and outbound directions. Appendix G provides a list of highly susceptible ports and services that should be blocked or limited as much as possible without adversely affecting customer requirements.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET FW 8551.1 & Appendix C: Review the rules and filters applied to all interfaces of the firewall for both inbound and outbound directions to ensure that the firewall policy is IAW with DOD 8551.1 Ports, Protocols and Services and Appendix C.

###Fixes###

NET FW 8551.1 & Appendix C: Have the firewall administrator make the appropriate changes so tha the policy is IAW DOD 8551.1 and Appendix C of the Network Infrastructure STIG.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1163 CAT: 1 Ensure that the Enclave perimeter is protected.

Router Type:

Target(s): Firewall - Data Network

8500.2 IA Control: ECSC-1

Category: 4.3 - Firewall

Condition(s): Firewall - Data Network

Vulnerability The IAO will ensure that the Enclave perimeter is protected

Vulnerability Discussion: Access Control Lists (ACLs) and firewalls are the first line of defense in a layered security approach. They permit authorized packets and deny unauthorized packets based on port or service type. They enhance the posture of the network by not allowing packets to even reach a potential target within the security domain. The list provided are highly susceptible ports and services that should be blocked or limited as much as possible without adversely affecting customer requirements. Auditing packets attempting to penetrate the network but are stopped by an ACL will allow network administrators to broaden their protective ring and more tightly define the scope of operation.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

Perimeter Protection: If a firewall has not been implemented to protect the entire facility, than the perimeter router must be configured with a deny-by-default policy.

Review the rules and filters applied to all interfaces of the inbound and outbound directions to ensure that the policy is IAW with DOD 8551.1 Ports, Protocols and Services and Appendix C.

###Fixes###

Perimeter Protection: The site must have either a firewall to protect the entire facility OR the perimeter router must be configured with a deny-by-default policy.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1170 CAT: 3 A firewall is being used that has not attained the

Router Type:

Target(s): Firewall - Data Network

8500.2 IA Control: DCAS-1: DCSR-1: DCSR-2: DCSR-3: ECSC-1

Category: 4.3 - Firewall

Condition(s): Firewall - Data Network

Vulnerability The IAM will ensure that only firewalls that have a Common Criteria Protection Profile evaluation of EAL4 or greater are placed in the network infrastructure.

Vulnerability Discussion: With the massive amount of firewall vendors on the market, the only assurance that the firewall meets or exceeds the minimum security requirements obtained in the Enclave Security Policy and the Network Infrastructure STIG is the Common Criteria EAL4 rating.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

Firewall EAL4 by NIST: Have the firewall or network administrator provide a copy of the common criteria award provided from the vendor.

Search http://niap.nist.gov/cc-scheme/vpl/vpl_type.html for current ratings.

###Fixes###

Firewall EAL4 by NIST: The NSO needs to incorporate a Common Criteria EAL4 rated firewall into the perimeter defenses.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1180 CAT: 2 A screened subnet (DMZ) is not implemented.

Router Type:

Target(s): Firewall - Data Network

8500.2 IA Control: EBBD-1: EBBD-2: EBBD-3: ECSC-1

Category: 4.4 - DMZ

Condition(s): Firewall - Data Network

Vulnerability The IAO/NSO will ensure that a Screened Subnet (DMZ) Firewall Architecture is implemented.

Vulnerability Discussion: Without the Dual-Homed screened subnet (DMZ) architecture traffic that would be normally destined for the DMZ would have to be redirected to the sites internal network. This would allow for a greater opportunity for hackers to exploit.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET FW DMZ Architecture: Verify this requirement by inspecting the site network topology and firewall interface configurations.

###Fixes###

NET FW DMZ Architecture: NSO needs to incorporate the Dual-Homed with screened subnet(DMZ) architecture into the sites architecture.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1190 CAT: 2 Using an application-level firewall

Router Type:

Target(s): Firewall - Data Network

8500.2 IA Control: ECSC-1

Category: 4.9 - Proxies

Condition(s): Firewall - Data Network

Vulnerability The IAO/NSO will ensure that all networks use application-level gateways or firewalls to proxy all traffic to external networks. Web proxy services will be provided as a minimum.

NOTE: Due to technological advances there are devices such as SSL Gateways, E-mail Gateways, etc., that will proxy services to protect the enclave. Therefore, a layer 4 or stateful inspection firewall, in collaboration with application level proxy devices to service all connections, is an acceptable alternative.

Vulnerability Discussion: Application-level proxy firewalls screen traffic to verify the traffic is secure for all connections. Allowing any lesser form of security enforcement allows for possible avenues of attack, and also will not allow for the enforcement of the Enclave Security Policy.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET FW Application Proxies: Review the firewall specification sheet.

###Fixes###

NET FW Application Proxies: The site architecture needs to deploy an application-level firewall to allow for screening of all traffic bi-directionally. This can be accomplished either of two ways:

1. An application-level firewall at the perimeter to protect the whole Enclave to include the Security Domains.

2. A non application-level firewall at the perimeter (e.g., stateful inspection, hybrid, packet-filter) with an application-level firewall protecting every Security Domain with no IP addressable systems or devices operating in the area between the non application-level firewall and the Security Domains firewall.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1200 CAT: 2 Firewall placement is not IAW the Network STIG.

Router Type:

Target(s): Router

8500.2 IA Control: EBBD-1: EBBD-2: EBBD-3: ECSC-1

Category: 4.3 - Firewall

Condition(s): Router

Vulnerability The IAO/NSO will ensure, when protecting the boundaries of a network, the firewall is placed between the private network and the perimeter router and the DMZ.

Vulnerability Discussion: The only way to mediate the flow of traffic between the inside network, the outside connection, and the DMZ is to place the firewall into the architecture in a manner that allows the firewall the ability to screen content for all three destinations.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET Firewall Location: Inspect the network topology diagrams and visually trace the firewall connections.

###Fixes###

NET Firewall Location: Move the firewall into the prescribed location to allow for enforcement of the Enclave Security Policy and allow for all traffic to be screened.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1220 CAT: 2 Firewall needs to provide authentication.

Router Type:

Target(s): Firewall - Data Network

8500.2 IA Control: ECSC-1: IAIA-1: IAIA-2

Category: 1.3 - Identity Management

Condition(s): Firewall - Data Network

Vulnerability The IAO/NSO will ensure the firewall authenticates all administrators using individual accounts before granting access to the firewall's administration interface.

Vulnerability Discussion: Firewalls are the enforcement mechanisms of the security policy making it an ideal candidate for attack. Its placement in the network and the level of access granted to the users accessing the device also increases the risk associated with remote management. For this reason all personnel that access the firewall both local and remotely must have the minimum privilege level needed for them to perform their duties. The standard 3 attempt lockout is enforced, with the exception that when an firewall administrator is locked out the NSO is responsible for unlocking the account. If the firewall is not compliant with the DoD PKI then deployment of needed resources will be hindered and could result in a Denial of Services for some personnel.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET Firewall Authentication: Review the local policy that states this requirement and verify by review of the access logs on the firewall.

###Fixes###

NET Firewall Authentication: Configure the firewall to require individual authentication before granting access to the firewall administrative interface.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1222 CAT: 2 Administrators weuse lowest privilege level.

Router Type:

Target(s): Firewall - Data Network

8500.2 IA Control: ECSC-1

Category: 2.2 - Least Privilege

Condition(s): Firewall - Data Network

Vulnerability The IAO/NSO will ensure all user and administrator accounts are assigned the lowest privilege level that allows them to perform their duties.

Vulnerability Discussion: Firewalls are the enforcement mechanisms of the security policy making it an ideal candidate for attack. Its placement in the network and the level of access granted to the users accessing the device also increases the risk associated with remote management. For this reason all personnel that access the firewall both local and remotely must have the minimum privilege level needed for them to perform their duties.

References: Network Infrastructure Security Implementation Guide

Checks/Fixes: ###Checks###

Firewall Least Privilege: Have the FA display the user database on the firewall.

###Fixes###

Firewall Least Privilege: Change the privileges assigned to administrators to the lowest privilege level that allows them to perform their duties.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1224 CAT: 3 Firewall configure to lock out after 3 attempts

Router Type:

Target(s): Firewall - Data Network

8500.2 IA Control: ECLO-1: ECLO-2: ECSC-1

Category: 1.1 - Passwords

Condition(s): Firewall - Data Network

Vulnerability The IAO/NSO will ensure the firewall is set to lock out accounts after three unsuccessful logon attempts.

Vulnerability Discussion: Firewalls are the enforcement mechanisms of the security policy making it an ideal candidate for attack. Its placement in the network and the level of access granted to the users accessing the device also increases the risk associated with remote management. The standard 3 attempt lockout is enforced, with the exception that when an firewall administrator is locked out the NSO is responsible for unlocking the account.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET FW Logon Attempts 3: Have the firewall administrator demonstrate that an account will lock out after three attempts.

###Fixes###

NET FW Logon Attempts 3: Have the FA change the configuration settings to enforce the 3 unsuccessful logon attempts.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1226 CAT: 2 Firewall remote access is not restricted

Router Type:

Target(s): Firewall - Data Network

8500.2 IA Control: ECPA-1: ECSC-1

Category: 1.3 - Identity Management

Condition(s): Firewall - Data Network

Vulnerability The IAO/NSO will ensure that only the FA is allowed to remotely access the firewall administration interface.

Vulnerability Discussion: Firewalls are the enforcement mechanisms of the security policy making it an ideal candidate for attack. For this reason all personnel that access the firewall remotely must have be limited.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET FW Remote Access: Review the local policy that states this requirement and the firewall configuration.

###Fixes###

NET FW Remote Access: Change the privileges assigned to administrators so that only the senior FA can access the firewall remotely.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1228 CAT: 2 Firewall administration by unauthorized personnel

Router Type:

Target(s): Firewall - Data Network

8500.2 IA Control: ECSC-1: IAAC-1

Category: 1.3 - Identity Management

Condition(s): Firewall - Data Network

Vulnerability The IAO/NSO will ensure only authorized personnel have permission to change security settings on the firewall.

Vulnerability Discussion: Firewalls are the enforcement mechanisms of the security policy making it an ideal candidate for attack. For this reason all personnel that access the firewall must have the minimum privilege level needed for them to perform their duties.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET FW Authorized Admin: Review the local policy that states this requirement and verify by review of the access logs on the firewall.

###Fixes###

NET FW Authorized Admin: Change the privileges assigned to administrators to the lowest privilege level that allows them to perform their duties.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1240 CAT: 2 Firewall is not configured to protect the network.

Router Type:

Target(s): Firewall - Data Network

8500.2 IA Control: DCBP-1: ECSC-1

Category: 4.3 - Firewall

Condition(s): Firewall - Data Network

Vulnerability The IAO/NSO will ensure that the firewall is configured to protect the network against denial of service attacks such as Ping of Death, TCP SYN floods, etc.

Vulnerability Discussion: A SYN-flood attack is a denial-of-service attack where the attacker send a huge amount of please-start-a-connection packets and then nothing else. This causes the device being attacked to be overloaded with the open sessions and eventually crash.

A ping sweep (also known as an ICMP sweep) is a basic network scanning technique used to determine which of a range of IP addresses map to live hosts (computers).

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET FW Protection Policies: Have the FW administrator show you the FW configuration files and rules to verify that compliance of this requirement.

CAVEAT: If the site has implemented SYN flood protection for the network using the premise router, it is not an additional requirement to implement this on the firewall.

###Fixes###

NET FW Protection Policies: If the firewall support SYN-flood or ping sweep protection then enable these features. If the firewall does not support these features, enable the security features on the router to protect the network from these attacks.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1250 CAT: 2 Firewall has unnecessary services enabled.

Router Type:

Target(s): Firewall - Data Network

8500.2 IA Control: ECSC-1

Category: 4.3 - Firewall

Condition(s): Firewall - Data Network

Vulnerability The FA will ensure the firewall does not utilize or enable any services (DNS, HTTP, etc.) not required by the firewall engine.

Vulnerability Discussion: The additional services that the firewall has enabled increases the risk for an attack since the firewall will listen for these services. In addition, these services provide an unsecured method for an attacker to gain access to the router.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET FW Unnecessary Services: Have the FA display the services running on the firewall appliance or underlying OS.CAVEAT: Anti-virus software running on the firewall's OS would be an exception to the above requirement. In fact, it is recommended that anti-virus software be implemented on any non-appliance firewall if supported. However, it is not a finding if anti-virus software has not been implemented.

###Fixes###

NET FW Unnecessary Services: The Firewall Administrator will only utilize services related to the operation of the firewall and even if they are part of the firewall standard suite, they will be uninstalled or disabled.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1252 CAT: 2 Firewall version is not a supported or current.

Router Type:

Target(s): Firewall - Data Network

8500.2 IA Control: DCSL-1: ECSC-1

Category: 3.1 - Security Patches

Condition(s): Firewall - Data Network

Vulnerability The FA will use a supported version of the firewall software with all security-related patches applied.

Vulnerability Discussion: Unsupported versions will lack security enhancements as well as support provided by the vendors to address vulnerabilities.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET FW Patch Mgt: Verify firewall release and maintenance level and research the vendors vulnerability list and upgrade database.

###Fixes###

NET FW Patch Mgt: The firewall administrator will install all version updates and security patches in a timely manner.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1254 CAT: 2 Firewall is not operating on a STIG'd OS

Router Type:

Target(s): Firewall - Data Network

8500.2 IA Control: DCCS-1: DCCS-2: ECSC-1

Category: 12.4 - CM Process

Condition(s): Firewall - Data Network

Vulnerability The FA will ensure that if the firewall product operates on an OS platform, the host must be STIG compliant prior to the installation of the firewall product.

Vulnerability Discussion: If the host that a firewall engine is operating on is not secured, the firewall itself is exposed to greater risk.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET FW STIG OS platform: Review documentation that the OS was STIG compliant prior to firewall installation and that the appropriate patches have been applied that address all IAVAs.

###Fixes###

NET FW STIG OS Platform: The firewall administrator will install all patches that address IAVA.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1260 CAT: 3 Firewall admin must register with vendor

Router Type:

Target(s): Firewall - Data Network

8500.2 IA Control: ECSC-1

Category: 3.1 - Security Patches

Condition(s): Firewall - Data Network

Vulnerability The FA will subscribe to the vendor's vulnerability mailing list to be made aware of required upgrades and patches.

Vulnerability Discussion: Not being on the vendors vulnerability list can lead to the firewall software not being updated when a new release or security patch is released by the vendor.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET FW Vendor Mail List: Interview the FA for compliance.

###Fixes###

NET FW Vendor Mail List: Have the FA subscribe to the vendors vulnerability mailing list.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1280 CAT: 3 The firewall logs are not being reviewed daily.

Router Type:

Target(s): Firewall - Data Network

8500.2 IA Control: ECAT-1: ECAT-2: ECSC-1

Category: 10.3 - Review

Condition(s): Firewall - Data Network

Vulnerability The IAO/NSO will ensure there is a review on a daily basis, of the firewall log data by the firewall administrator (FA), or other qualified personnel, to determine if attacks or inappropriate activity has occurred.

Vulnerability Discussion: A firewall should be the first line of defense for any network. The firewall logs can be used for forensic analysis in support of incident as well as to aid with normal traffic analysis. It can take numerous days to recover from a firewall outage when a proper backup scheme is not used.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET FW Review Logs Daily: Review site policy, then interview FW administrator and authorized personnel with FW access to determine compliance.

###Fixes###

NET FW Review Logs Daily: Insure that the NSO or FA reviews the firewall logs daily.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1282 CAT: 3 Firewall log retention does not meet policy.

Router Type:

Target(s): Firewall - Data Network

8500.2 IA Control: ECRR-1: ECSC-1

Category: 10.5 - Retention

Condition(s): Firewall - Data Network

Vulnerability The FA will ensure the firewall logs are retained online for a minimum of 30 days and then stored offline for one year.

Vulnerability Discussion: A firewall should be the first line of defense for any network. The firewall logs can be used for forensic analysis in support of incident as well as to aid with normal traffic analysis. It can take numerous days to recover from a firewall outage when a proper backup scheme is not used.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET FW Log Retention: Interview FW administrator and ask how long logs are maintained offline. Inspect the firewall configuration to determine how long logs files are retained online.

###Fixes###

NET FW Log Retention: Archive log data on the firewall for 30 days and keep offline for a minimum of one year.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1284 CAT: 3 The firewall configuration is not backed up weekly

Router Type:

Target(s): Firewall - Data Network

8500.2 IA Control: CODB-1: CODB-2: CODB-3: ECSC-1

Category: 13.4 - Backup & Recovery

Condition(s): Firewall - Data Network

Vulnerability The IAO/NSO will ensure the firewall configuration data are backed up weekly and whenever configuration changes occur.

Vulnerability Discussion: A firewall should be the first line of defense for any network. The firewall logs can be used for forensic analysis in support of incident as well as to aid with normal traffic analysis. It can take numerous days to recover from a firewall outage when a proper backup scheme is not used.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET FW Config BU Weekly: Review site policy and interview FW administrator.

###Fixes###

NET FW Config BU Weekly: Back up firewall configuration data on a weekly basis.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1286 CAT: 3 The firewall logs are not backed up weekly

Router Type:

Target(s): Firewall - Data Network

8500.2 IA Control: ECSC-1: ECTB-1

Category: 13.4 - Backup & Recovery

Condition(s): Firewall - Data Network

Vulnerability The IAO/NSO will ensure the firewall log data is backed up weekly.

Vulnerability Discussion: A firewall should be the first line of defense for any network. The firewall logs can be used for forensic analysis in support of incident as well as to aid with normal traffic analysis. It can take numerous days to recover from a firewall outage when a proper backup scheme is not used.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET FW Log BU Weekly: Review site policy and interview FW administrator.

###Fixes###

NET FW Log BU Weekly: Backup firewall logs on a weekly basis.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1290 CAT: 2 The firewall is not configured to alarm the admini

Router Type:

Target(s): Firewall - Data Network

8500.2 IA Control: ECSC-1

Category: 4.3 - Firewall

Condition(s): Firewall - Data Network

Vulnerability The IAO/NSO will ensure the firewall is configured to alert the administrator of a potential attack or system failure.

Vulnerability Discussion: The first device that is under the sites control that has the possibility to alarm the local staff of an ongoing attack is the firewall. The local site generally does not have access to the JID logs so the firewall alarms would be the first indication of an attack or system failure.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET FW Alerts: Review the firewall configuration to determine what alerts have been defined and how the notifications are performed.

###Fixes###

NET FW Alerts: Configure the firewall to alarm the FA of potential attacks or system failure.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1300 CAT: 3 The firewall is not configured properly.

Router Type:

Target(s): Firewall - Data Network

8500.2 IA Control: ECAR-1: ECAR-2: ECAR-3: ECSC-1

Category: 10.2 - Content Configuration

Condition(s): Firewall - Data Network

Vulnerability The FA will ensure the following capabilities will be enabled on the firewall:

Log unsuccessful authentication attempts.

Stamp audit trail data with the date and time when recorded.

Record the Source IP, Destination IP, protocol used, and the action taken.

Log administrator logons, changes to the administrator group, and account lockouts.

Protect audit logs from deletion and modification.

The firewall will provide the ability to record a readable audit log of security-related events, with accurate dates and times, with the capability to search and sort the audit log based on relevant attributes.

Vulnerability Discussion: The firewall and the associated logging functions allows for forensic investigations if properly configured and protected. The administrators account is the most sought after account so extra protection must be taken to protect this account.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET FW Config Capabilities: Have the FA display the logging configuration. Review log data created by firewall. Review log data created by firewall. Have the FA display the logging configuration and review the log data. Have the FA display the configuration setting that enables this function. Review log data created by firewall and the reporting capabilities.

###Fixes###

NET FW Config Capabilities: Ensure that the firewall logs unsuccessful authentication attempts. Ensure that the firewall stamps audit trail data with the date and time. Ensure that the firewall records the Source IP, Destination IP, protocol used, and the actions taken. Ensure that the firewall logs administrator logons, changes to the administrator group, and account lockouts. Ensure that the firewall protects audit logs from deletion and modification. Ensure that the firewall provides a means to record a readable audit trail of security related events. Ensure the FA incorporates the security requirements from section 3.4.2.2 of the Network Infrastructure STIG into the remote management of the firewall.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1310 CAT: 2 Use of in-band management is not limited.

Router Type:

Target(s): Firewall - Data Network

8500.2 IA Control: ECND-1: ECND-2: ECSC-1

Category: 4.3 - Firewall

Condition(s): Firewall - Data Network

Vulnerability The FA will limit the use of in-band management to situations where the use of OOB management would hinder operational commitments or when emergency situations arise.

Vulnerability Discussion: It is imperative that communications used for administrative access to firewalls is limited to emergency situations or where out-of-band management would hinder daily operational requirements. In-band management introduces the risk of an attacker gaining access to the firewall internally or even externally.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET FW In-band is not limited: Interview the IAO/NSO and FA for compliance

###Fixes###

NET FW In-band is not limited: Use out-of-band management.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1312 CAT: 2 Two-factor authentication is not used for in-band

Router Type:

Target(s): Firewall - Data Network

8500.2 IA Control: ECSC-1: IAAC-1: IAIA-1: IAIA-2

Category: 1.4 - Authentication Services

Condition(s): Firewall - Data Network

Vulnerability For in-band management, the IAO/NSO will implement the use of two factor authentication.

Vulnerability Discussion: Without strong two-factor authorization, unauthorized users may gain access to the firewall that could lead to the entire network being compromised.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET FW Two-factor Authen: Interview the IAO/NSO and FA for compliance, then have the FA establish a management session to determine compliance.

###Fixes###

NET FW Two-factor Authen: The firewall and authentication servers will be configured so that all authorized users are forced to use two-factor authentication.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1314 CAT: 2 In-band management is not restricted.

Router Type:

Target(s): Firewall - Data Network

8500.2 IA Control: ECND-1: ECND-2: ECSC-1

Category: 4.3 - Firewall

Condition(s): Firewall - Data Network

Vulnerability The FA will ensure that the use of in-band management is restricted to a limited number of authorized IP addresses.

Vulnerability Discussion: Without limited in-band management connections, unauthorized users may gain access to the firewall and could then compromise the entire network.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET FW In-band Limited: Examine the firewall configuration to determine what IP addresses are permitted access via telnet or SSH.

###Fixes###

NET FW In-band Limited: For in-band management, the FA will configure the network device to restrict the use of in-band connections equal to or less than the number of firewall administrators.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1316 CAT: 2 In-band management must meet FIPS 140-2.

Router Type:

Target(s): Firewall - Data Network

8500.2 IA Control: ECNK-1: ECSC-1

Category: 8.1 - Encrypted Data in Transit

Condition(s): Firewall - Data Network

Vulnerability The FA will ensure that all in-band management access to all firewalls is secured using FIPS 140-2 validated encryption such as AES, 3DES, SSH, or SSL.

Vulnerability Discussion: Without encrypted in-band management connections, unauthorized users may gain access to firewalls. If any firewalls are compromised, the entire network could also be compromised.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET FW In-band must use SSH: Examine all firewall configurations to verify that only SSH connections are permitted access.

###Fixes###

NET FW In-band must use SSH: For in-band management the FA will configure the firewall to only allow SSH connections.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1325 CAT: 2 An external NIDS has not been implemented.

Router Type:

Target(s): IDS / IPS

8500.2 IA Control: DCCS-2: ECSC-1

Category: 4.5 - IDS

Condition(s): IDS / IPS

Vulnerability If an NID is required by the CNDSP, the IAO/NSO will ensure that an external NIDS is installed and implemented so that all external connections can be monitored.

Vulnerability Discussion: The incorrect placement of the external NIDS may allow unauthorized access to go undetected and limit the ability of security personnel to stop malicious or unauthorized use of the network.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET IDS CNDSP Required: CAVEAT: If a site does not have a direct link to a NIPRNet or SIPRNet node router—that is, its connection to the NIPRNet or SIPRNet is through an upstream link to another activity's premise router, then this site would not be required to have its own external NIDS, if the upstream activity has an external NIDS that is being monitored by the RCERT or a certified CND Service Provider. However, if this site has other external connections such as an Internet Service Provider, this traffic would need to be monitored by a CND Service Provider using an external NIDS.

Procedure: Inspect the network topology to verify compliance.

###Fixes###

NET IDS CNDSP Required: Place the external NIDS on the exterior of the network in front of the premise router so that it can monitor all external connections.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1326 CAT: 2 External NIDS is not being monitored by the CNDSP

Router Type:

Target(s): IDS / IPS

8500.2 IA Control: DCCS-2: ECSC-1

Category: 4.5 - IDS

Condition(s): IDS / IPS

Vulnerability If a NID is required by the CNDSP, the IAO/NSO will ensure that the certified CNDSP is continuously monitoring the data from the external NIDS.

Vulnerability Discussion: In order to ensure that an attempted or existing attack doesnt go unnoticed, the data from the sensors must be monitored continuously.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET IDS CNDSP Monitoring: Have the IAO/NSO provide the agreement from a certified CND Service Provider outlining their responsibilities.

###Fixes###

NET IDS CNDSP Monitoring: Insure that the data is continuously being monitored by the CND Service Provider.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1327 CAT: 2 NIDS is not located between the POP and Premise.

Router Type:

Target(s): IDS / IPS

8500.2 IA Control: DCCS-2: ECSC-1

Category: 4.5 - IDS

Condition(s): IDS / IPS

Vulnerability The IAO/NSO will ensure that the external NIDS is located between the site's NIPRNet or SIPRNet Point of Presence (POP) and the premise router.

Vulnerability Discussion: The incorrect placement of the external NIDS may allow unauthorized access to go undetected and limit the ability of security personnel to stop malicious or unauthorized use of the network. In order to ensure that an attempted or existing attack goes unnoticed, the data from the sensors must be monitored continuously

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET IDS Location: Inspect the network topology and physical connectivity to verify compliance.

###Fixes###

NET IDS Location: The external NIDS must be placed between the sites NIPRNet or SIPRNet POP and the premise router.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1328 CAT: 3 IDS data is being monitored unauthorized persons.

Router Type:

Target(s): IDS / IPS

8500.2 IA Control: DCCS-2: ECSC-1

Category: 4.5 - IDS

Condition(s): IDS / IPS

Vulnerability The IAO/NSO will ensure that the data from the external NIDS is restricted to CNDSP personnel only.

Vulnerability Discussion: The external NIDS is monitoring all traffic on the external connections. It is imperative that this traffic is only reviewed and monitored by trusted and authorized personnel with a need to know.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET IDS Authorized Reviewers: Have the IAO/NSO provide copies of the authorization letter assigning the reviews.

###Fixes###

NET IDS Authorized Reviewers: The IAO will ensure that the monitoring of the external IDS will be performed by the RCERT or a certified CND Service Provider.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1330 CAT: 2 The NIDS is not monitoring all traffic that enters

Router Type:

Target(s): IDS / IPS

8500.2 IA Control: EBBD-1: EBBD-2: EBBD-3: ECSC-1

Category: 4.5 - IDS

Condition(s): IDS / IPS

Vulnerability The Network IDS administrator will ensure a Network IDS is installed and operational with all connections (e.g., LAN and WAN) being monitored.

Vulnerability Discussion: Although the firewall has logging functions, the first device dedicated to the detection and response of intruders and malicious activities is the Network Intrusion Detection System (NID). This NID provides the site with near real time alarms using known attack signatures and anomaly detection.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET IDS Internal Location: Note: If monitoring is being performed using a switch SPAN port, it is recommended that the IDS is configured in Stealth Mode—the NIC connected to the SPAN port would not have any network protocol stacks bound to it. A second NIC would then be connected to an OOB network. Stealth mode will eliminate the risk of the IDS itself being attacked. Stealth mode would not be applicable if the IDS is monitoring from a network tap solution. The second NIC is for the IDS sensor to be able to backhaul its data via the out-of-band connection to the IDS manager. The sensors need to talk to the manager, so if your sensors are in stealth mode, there is no way to reach the manager on the in-band network.

Procedure: Review the network topology diagrams and equipment.

###Fixes###

NET IDS Internal Location: The NSO needs to incorporate a NID into the site architecture IAW the Network Infrastructure STIG.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1340 CAT: 2 The NSO does not have an incident response policy.

Router Type:

Target(s): IDS / IPS

8500.2 IA Control: ECSC-1: VIIR-1: VIIR-2

Category: 10.1 - Procedures

Condition(s): IDS / IPS

Vulnerability The IAO/NSO will establish policies outlining procedures to notify JTF GNO when suspicious activity is observed.

Vulnerability Discussion: A network intrusion system is a policy enforcement mechanism that the site must sue to enforce the Enclave Security Policy. If a clear policy has not be established for reporting suspicious activity to the RCERT, then the site, and possibly all of DoD, is at a greater risk for exposure.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET IDS Internal Policies: Have the IAO/NSO provide a copy of the policy outlining procedures to notify the CERT of suspicious activity.

###Fixes###

NET IDS Internal Policies: Develop an incident response policy and a procedure to carry out the policy.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1342 CAT: 2 The NID reviewers have not been authorized by the

Router Type:

Target(s): IDS / IPS

8500.2 IA Control: ECAN-1: ECSC-1

Category: 2.2 - Least Privilege

Condition(s): IDS / IPS

Vulnerability The IAO/NSO will ensure that authorized reviewers of Network IDS data are identified in writing by the site's IAM.

Vulnerability Discussion: To preserve the chain of custody for possible legal action, all reviewers of the NID data must be have an authorization letter from the site commander outlining the individuals need to know.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET IDS Internal Auth Users: Have the IAO/NSO provide a copy of the letter identifying authorized reviewers.

###Fixes###

NET IDS Internal Auth Users: Have the site commander sign a authorization letter for all individuals that are required to review the NID data. Ensure that only authorized personnel have access to the IDS data.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1344 CAT: 2 Unauthorized traffic is not logged.

Router Type:

Target(s): IDS / IPS

8500.2 IA Control: ECAT-1: ECAT-2: ECSC-1

Category: 10.2 - Content Configuration

Condition(s): IDS / IPS

Vulnerability The IAO/NSO will ensure that any unauthorized traffic is logged for further investigation.

Vulnerability Discussion: Audit logs are necessary to provide a trail of evidence in case the network is compromised. With this information, the network administrator can devise ways to block the attack and possibly identify and prosecute the attacker. Information supplied by an IDS can be used for forensic analysis in support of incident as well as to aid with normal traffic analysis.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET IDS Internal Logging: Have the IAO/NSO display the logging and auditing features of the NID.

###Fixes###

NET IDS Internal Logging: Configure the IDS to log all unauthorized or suspicious traffic.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1346 CAT: 2 NSO has not established weekly backup procedures

Router Type:

Target(s): IDS / IPS

8500.2 IA Control: CODB-1: CODB-2: CODB-3: ECSC-1

Category: 12.9 - Documentation

Condition(s): IDS / IPS

Vulnerability The IAO/NSO will establish weekly data backup procedures for the Network IDS.

Vulnerability Discussion: IDS data needs to be backed up to insure that the IDS data is preserved in the event of a hardware failure of the IDS or the IDS could be breached.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET IDS Backups: Verify the IAO/NSO has established weekly backup procedures for IDS data.

###Fixes###

NET IDS Backups: The NSO has not established weekly backup procedures.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1348 CAT: 2 NSO has not established anti-virus updates procedu

Router Type:

Target(s): IDS / IPS

8500.2 IA Control: ECSC-1: ECVP-1

Category: 12.9 - Documentation

Condition(s): IDS / IPS

Vulnerability The IAO/NSO will establish anti-virus update procedures for the Network IDS.

Vulnerability Discussion: To preserve the integrity of the IDS information and its operational capability, it is imperative that anti-virus software is kept up to date.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET IDS Internal Virus Updates: Verify the IAO/NSO has established anti-virus updates procedures

###Fixes###

NET IDS Internal Virus Updates: NSO must establish anti-virus updates procedures

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1350 CAT: 3 SA has not subscribed to the vendor notifications.

Router Type:

Target(s): IDS / IPS

8500.2 IA Control: ECSC-1

Category: 4.5 - IDS

Condition(s): IDS / IPS

Vulnerability The Network IDS administrator will subscribe to the vendor's vulnerability mailing list.

The Network IDS administrator will update the Network IDS when software is provided by Field Security Operations for the RealSecure distribution, and for all other Network IDS software distributions when a security-related update is provided by the vendor.

Vulnerability Discussion: Keeping the NID software updated with the latest engine and attack signatures will allow for the NID to detect all forms of known attacks. Not maintaining the NID properly could allow for attacks to go unnoticed.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET IDS Internal Updates: Have the SA display update notifications that have been received to determine compliance.

Have the NID SA display the build number or patch level, then search the vendor's vulnerability database for current release and patch level.

###Fixes###

NET IDS Internal Updates: Have the NID administrator subscribe to the X-press notification or similar service offered by the vendor.

Ensure the NID software is updated when software is available either by FSO or the vendor for security related distributions.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1362 CAT: 2 Switches and associated cross-connect hardware are

Router Type:

Target(s): Layer 2 Switch; Layer 3 Switch

8500.2 IA Control: ECSC-1

Category: 5.9 - Device Locations

Condition(s): Layer 3 Switch: Layer 2 Switch

Vulnerability The IAO/NSO will ensure that all switches and associated cross-connect hardware are kept in a secured IDF or an enclosed cabinet that is kept locked.

Vulnerability Discussion: Since the IDF includes all hardware required to connect horizontal wiring to the backbone wiring, it is imperative that all switches and associated cross-connect hardware are kept in a secured IDF or an enclosed cabinet that is kept locked. This will also prevent an attacker from gaining privilege mode access to the switch. Several switch products only require a reboot of the switch in order to reset or recover the password.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET SW Location: Visual inspect data closets and verify the closet is locked or if located in an open area that the equipment resides in a secured cabinet.

###Fixes###

NET SW Location: The IAO will ensure that all unused data outlets are detached from the network infrastructure or electronically disabled from the network infrastructure in all communications closets.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1364 CAT: 2 Site does not utilize TACACS+, RADIUS, or other DO

Router Type:

Target(s): Layer 2 Switch; Layer 3 Switch

8500.2 IA Control: DCCS-2: ECSC-1

Category: 1.4 - Authentication Services

Condition(s): Layer 2 Switch: Layer 3 Switch

Vulnerability The IAO/NSO will ensure that an authentication server is used to gain administrative access to all switches.

Vulnerability Discussion: Without TACACS+ or approved Authentication Server, unauthorized users may gain access and possibly control of the switch. If the switched network is compromised, large portions of the network could be incapacitated with only a few commands.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET SW Authentication Access: Reference router procedure guide

###Fixes###

NET SW Authentication Access: The switch administrator will configure the TACACS+ server with standard accounts and user passwords. The switch administrator will ensure that standard accounts are not created directly on the switch. The switch administrator will ensure that the site uses RADIUS, TACACS+, or other DOD approved device for remote administrative access to the switch.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1365 CAT: **2** More than one emergency account has been defined.

Router Type:

Target(s): Layer 2 Switch; Layer 3 Switch

8500.2 IA Control: DCCS-2: ECSC-1

Category: 1.3 - Identity Management

Condition(s): Layer 2 Switch: Layer 3 Switch

Vulnerability The IAO/NSO will ensure that when an authentication server is used for administrative access to the switch, only one account can be defined locally on the switch for use in an emergency (i.e., authentication server or connection to the server is down).

Vulnerability Discussion: Authentication for administrative access to the switch is required at all times. A single account can be created on the switchs local database for use in an emergency such as when the authentication server is down or connectivity between the router and the authentication server is not operable.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET SW Local Accounts: Reference procedure guide

###Fixes###

NET SW Local Accounts: Ensure that only one local account has been defined on the switch and store the username and password in a secured manner.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1366 CAT: **1** Group accounts or user accounts without passwords

Router Type:

Target(s): Layer 2 Switch; Layer 3 Switch

8500.2 IA Control: ECSC-1

Category: 1.3 - Identity Management

Condition(s): Layer 2 Switch: Layer 3 Switch

Vulnerability The IAO/NSO will ensure that each user has their own account to access the switch with username and password.

Vulnerability Discussion: Without passwords on user accounts, one level of complexity is removed from gaining access to the switches. If a default userid has not been changed or is guessed by an attacker, the network could be easily compromised as the only remaining step would be to crack the password. Sharing group accounts on any switch is strictly prohibited. If these group accounts are not changed when someone leaves the group, that person could possibly gain control of the switch. Having group accounts does not allow for proper auditing of who is accessing or changing the network.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET SW No Group Accounts: Review the configuration for local accounts defined to the switch. If an authentication server is being used, examine those accounts with access to the switch.

###Fixes###

NET SW No Group Accounts: The switch administrator will ensure that all user accounts without passwords are removed. The switch administrator will ensure that individual user accounts are created for each authorized router administrator. The IAO will ensure that any group or duplicate account will be removed.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1367 CAT: 2 User accounts exist that are assigned higher privi

Router Type:

Target(s): Layer 2 Switch; Layer 3 Switch

8500.2 IA Control: ECSC-1

Category: 2.2 - Least Privilege

Condition(s): Layer 2 Switch: Layer 3 Switch

Vulnerability The IAO/NSO will ensure that all user accounts are assigned the lowest privilege level that allows them to perform their duties.

Vulnerability Discussion: By not restricting switch administrators to their proper privilege levels, access to restricted functions may be allowed before they are trained or experienced enough to use those functions. Network disruptions or outages could be caused by mistakes made by inexperienced administrators.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET SW Least Privilege: IOS Procedure: reference router procedure guide.

Catalyst Procedure: Check the accounts and their associated privilege levels configured in the authentication server. You can also use TACACS for even more granularity at the command level.

###Fixes###

NET SW Least Privilege: The switch administrator will assign switch accounts with the least privilege rule. Each user will have access to only the privileges they require to perform their respective duties. Access to the highest privilege levels should be restricted to a few users.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1368 CAT: 2 Unnecessary or unauthorized switch accounts exist.

Router Type:

Target(s): Layer 2 Switch; Layer 3 Switch

8500.2 IA Control: ECSC-1

Category: 1.3 - Identity Management

Condition(s): Layer 2 Switch: Layer 3 Switch

Vulnerability The switch administrator will immediately remove accounts from the authentication server or switch that are no longer required.

Vulnerability Discussion: Allowing unnecessary or unauthorized accounts may allow for them to be compromised by unauthorized users who could then gain full control of the switch. Denial of service, interception of sensitive information or other destructive actions could then take place.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET SW Expired Accounts: Verify that the site is in compliance by reviewing site's responsibilities list and reconcile this list with those accounts found in the switch's local database or authentication server.

###Fixes###

NET SW Expired Accounts: The switch administrator will ensure that procedures are in place to enforce proper account administration. The switch administrator will ensure that any account that is no longer needed will be disabled or removed from the system.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1369 CAT: 1 Type 5 encryption is not being used for passwords.

Router Type:

Target(s): Layer 2 Switch; Layer 3 Switch

8500.2 IA Control: ECSC-1

Category: 1.6 - Documentation and Storage

Condition(s): Layer 3 Switch: Layer 2 Switch

Vulnerability The IAO/NSO will ensure that passwords are not viewable when displaying the switch configuration.

Vulnerability Discussion: By allowing the use of the enable password command, which uses Type 7 encryption, the security provided by the TACACS+ server is bypassed. If unauthorized users gain access to the switches through the enable password they could gain full and unrestricted control of the switches. If the switch network is compromised, then large parts of the network could be incapacitated with only a few commands.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET SW PSW Type 5 encrypt: IOS Procedure: Review all Cisco switch configurations to ensure that an enable secret password is defined similar to the following example: enable secret 5 1rTsF$EdvjtWbi0qA2gXwyhetTb

Catalyst Procedure: Catalyst doesn't provide Type 5 thus this is an additional finding if the passwords are not disabled as referenced in NET1365.

###Fixes###

NET SW PSW Type 5 encrypt: The switch administrator will ensure that Type 5 (enable secret) encryption is used for password protection.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1380 CAT: 2 Switches are not password protected for OOB.

Router Type:

Target(s): Layer 2 Switch; Layer 3 Switch

8500.2 IA Control: EBRU-1: ECSC-1

Category: 1.3 - Identity Management

Condition(s): Layer 2 Switch: Layer 3 Switch

Vulnerability The IAO/NSO will ensure that all OOB management connections to the switch require passwords.

Vulnerability Discussion: Devices protected with weak password schemes or no password at all, provide the opportunity for anyone to crack the password or gain access to the device and cause network, device, or information damage or denial of service.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET SW OOB PSW protected: Interview the IAO/NSO to determine if the site is compliant with this requirement.

###Fixes###

NET SW OOB PSW protected: Access to the console does not require a password.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1381 CAT: 1 The console port is not configured to timeout the

Router Type:

Target(s): Layer 2 Switch; Layer 3 Switch

8500.2 IA Control: ECSC-1

Category: 4.7 - Routers

Condition(s): Layer 3 Switch: Layer 2 Switch

Vulnerability The switch administrator will ensure the switch console port is configured to time out after 10 minutes or less of inactivity.

Vulnerability Discussion: Switches have multiple areas of configuration. The more critical the area, the tighter the control should be. Setting the timeout of the session to ten minutes or less increases the level of protection afforded critical switches.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET SW Console Timeout: IOS procedure: Review each Cisco switch configuration to ensure that the console is disabled after 10 minutes of inactivity. The configuration should look similar to the following:line con 0login authentication admin_onlyexec-timeout 10 0

###Fixes###

NET SW Console Timeout: The network administrator will ensure that the timeout for unattended console port is set for no longer than 10 minutes via the exec-timeout command.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1382 CAT: 2 Modems are connected to the auxiliary or console p

Router Type:

Target(s): Layer 2 Switch; Layer 3 Switch

8500.2 IA Control: ECSC-1

Category: 4.10 - RAS

Condition(s): Layer 2 Switch: Layer 3 Switch

Vulnerability The IAO/NSO will ensure modems are not connected to the console or auxiliary ports.

Vulnerability Discussion: Access to the switch via a modem is potentially very risky. If an intruder were to gain access to the router via a modem, the potential for denial of service attacks, interception of sensitive information, and other destructive actions is greatly increased.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET SW Modems: Physically inspect any local switches to ensure modems are not connected.

###Fixes###

NET SW Modems: The network administrator will ensure that all modems connected to the switch are disconnected. Modems should only be connected for emergency maintenance.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1383 CAT: 3 Auxiliary ports are not disabled on all switches.

Router Type:

Target(s): Layer 2 Switch; Layer 3 Switch

8500.2 IA Control: ECSC-1

Category: 4.1 - Unneeded Ports, Protocols, and Services

Condition(s): Layer 2 Switch: Layer 3 Switch

Vulnerability The switch administrator will ensure that the switch's auxiliary port is disabled.

Vulnerability Discussion: The auxiliary port is typically used for remote administration via a modem. This, however, is seldom used and should therefore be disabled. Access to the switch via a modem is potentially very risky. If an intruder were to gain access to the switch via a modem, the potential for denial of service attacks, interception of sensitive information, and other destructive actions is greatly increased

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET SW Aux Disabled: View each switch's configuration to ensure that the auxiliary port is disabled with a configuration similar to the following:

line aux 0
no exec
transport input none

###Fixes###

NET SW Aux Disabled: The switch administrator will disable the auxiliary ports by using the following router commands:
line aux 0
no exec
transport input none

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1385 CAT: 1 Switches are not password protected for in-band ma

Router Type:

Target(s): Layer 2 Switch; Layer 3 Switch

8500.2 IA Control: ECSC-1

Category: 1.3 - Identity Management

Condition(s): Layer 2 Switch: Layer 3 Switch

Vulnerability The IAO/NSO will ensure that all in-band management connections to the switch require passwords.

Vulnerability Discussion: Devices protected with weak password schemes or no password at all, provide the opportunity for anyone to crack the password or gain access to the device and cause network, device, or information damage or denial of service.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET SW In-band Mgt PSW: Review each switch's configuration to ensure that the VTY ports require a login prompt. The configuration should look similar to the following:

```
line vty 0 4   login authentication admin_only
exec-timeout 10 0
transport input ssh
```

###Fixes###

NET SW In-band Mgt PSW: The site will ensure that all in-band management connections to the router require passwords.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1386 CAT: 2 In-band management is allowed to the switches from

Router Type:

Target(s): Layer 2 Switch; Layer 3 Switch

8500.2 IA Control: ECSC-1

Category: 4.7 - Routers

Condition(s): Layer 3 Switch: Layer 2 Switch

Vulnerability The switch administrator will ensure that the switch only allows in-band management sessions from authorized IP addresses from the internal network.

Vulnerability Discussion: Remote administration using VTY/telnet ports is inherently dangerous because anyone with a sniffer and access to the right LAN segment, can acquire the account and password information. With this intercepted information they could gain access to the switch and cause denial of service attacks, intercept sensitive information, or perform other destructive actions.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET SW In-band by Auth LAN: Review all configurations and verify that only authorized internal connections are allowed on VTY ports. The configuration should look similar to the following:

```
access-list 3   permit 192.168.1.10  log
access-list 3 permit 192.168.1.11 log
access-list 3 deny any

line vty 0 4
access-class 3 in
```

###Fixes###

NET SW In-band by Auth LAN: The network administrator will create an ACL for each switch that restricts the use of VTY ports for remote router administration, to only authorized internal connections. The ACL configuration should look similar to the following:

```
access-list 3 permit 215.17.1.0  0.0.0.255
access-list 3 permit 215.17.34.0  0.0.0.255
access-list 3 deny any
line vty 0 4
access-class 3 in
```

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1387 CAT: 2 Access to the switch is not restricted by valid en

Router Type:

Target(s): Layer 2 Switch; Layer 3 Switch

8500.2 IA Control: ECSC-1

Category: 8.1 - Encrypted Data in Transit

Condition(s): Layer 2 Switch: Layer 3 Switch

Vulnerability The switch administrator will ensure in-band management access to the switch is secured using FIPS 140-2 validated encryption such as AES, 3DES, SSH, or SSL.

Vulnerability Discussion: Remote administration using VTY/telnet ports is inherently dangerous because anyone with a sniffer and access to the right LAN segment can acquire the account and password information. With this intercepted information they could gain access to the switch and cause denial of service attacks, intercept sensitive information, or perform other destructive actions.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET SW In-band FIPS 140-2: Review all configurations and verify that only ssh is allowed on the VTY ports. The configuration should look similar to the following:

line vty 0 4
transport input ssh

###Fixes###

NET SW In-band FIPS 140-2: The network administrator will ensure that only validated encryption connections are allowed to access VTY ports.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1388 CAT: 2 Secure Shell timeout value is not 60 sec or less

Router Type:

Target(s): Layer 2 Switch; Layer 3 Switch

8500.2 IA Control: ECSC-1

Category: 4.7 - Routers

Condition(s): Layer 2 Switch: Layer 3 Switch

Vulnerability The switch administrator will set the SSH timeout value to 60 seconds, causing incomplete SSH connections to shut down after 60 seconds or less.

Vulnerability Discussion: Reducing the broken telnet session expiration time to 60 seconds or less strengthens the router from being attacked by use of an expired session.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET SW SSH 60 sec or less: Review the global configuration or have the router administrator execute the show ssh command on all of the switch routers to verify the timeout is set for 60 seconds or less.

###Fixes###

NET SW SSH 60 sec or less: Implement Secure Shell Timeout.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1389 CAT: 2 SSH Authentication retry value is greater 3.

Router Type:

Target(s): Layer 2 Switch; Layer 3 Switch

8500.2 IA Control: ECSC-1

Category: 1.3 - Identity Management

Condition(s): Layer 2 Switch: Layer 3 Switch

Vulnerability Secure Shell Authentication retry value is greater than 3.

Vulnerability Discussion: Setting the authentication retry to 3 or less strengthens against a Brute Force attack.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET SW Authention Retry 3: Review the global configuration or have the network administrator execute the show ssh command on all of the Cisco switches to verify the authentication retry is set for 3.

###Fixes###

NET SW Authention Retry 3: Implement Secure Shell Authentication retries.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1390 CAT: 2 Timeout for In-band must be 10 minutes or less.

Router Type:

Target(s): Layer 2 Switch; Layer 3 Switch

8500.2 IA Control: ECSC-1

Category: 4.7 - Routers

Condition(s): Layer 3 Switch: Layer 2 Switch

Vulnerability The IAO/NSO will ensure the timeout for in-band management access is set for no longer than 10 minutes.

Vulnerability Discussion: Switches have multiple areas of configuration. The more critical the area, the tighter the control should be. Setting the timeout of the session to ten minutes or less increases the level of protection afforded critical routers.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET SW In-band Timeout: Review each configuration to ensure that the VTY ports are disabled after 10 minutes of inactivity.

The configuration should look similar to the following:

```
line vty 0 4
login authentication admin_only
exec-timeout 10 0
transport input ssh
```

###Fixes###

NET SW In-band Timeout: The network administrator will ensure that the timeout for unattended telnet ports for no longer than 10 minutes via the exec-timeout command.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1391 CAT: 4 Logging of all in-band management access attempts

Router Type:

Target(s): Layer 2 Switch; Layer 3 Switch

8500.2 IA Control: ECSC-1

Category: 10.2 - Content Configuration

Condition(s): Layer 2 Switch: Layer 3 Switch

Vulnerability The switch administrator will configure the ACL that is bound to the VTY ports to log permitted and denied access attempts.

Vulnerability Discussion: Audit logs are necessary to provide a trail of evidence in case the network is compromised. Without an audit trail that provides a when, where, who and how set of information, repeat offenders could continue attacks against the network indefinitely. With this information, the network administrator can devise ways to block the attack and possibly identify and prosecute the attacker.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET SW In-band Logging: Review each configuration to ensure that all connection attempts to the VTY ports are logged.

```
access-list 3
permit 192.168.1.10 log
access-list 3 permit 192.168.1.11 log
access-list 3 deny any log.

line vty 0 4
access-class 3 in
```

###Fixes###

NET SW In-band Logging: The network administrator will add the log parameter to all access lists protecting the VTY ports. The configuration file should display lines similar to the following:

```
access-list 3 permit tcp host x.x.x.x any eq 23 log
access-list 3 deny any log

line vty 0 4
access-class 3 in
```

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1410 CAT: 2 The VLAN1 is being used for management traffic.

Router Type:

Target(s): Layer 2 Switch; Layer 3 Switch

8500.2 IA Control: ECSC-1

Category: 14.5 - Physical Layer Security

Condition(s): Layer 3 Switch: Layer 2 Switch

Vulnerability The IAO/NSO will ensure VLAN1 is not used for in-band management traffic. The IAO/NSO will assign a dedicated management VLAN to keep management traffic separate from user data and control plane traffic.

Vulnerability Discussion: All ports, including the internal sc0 interface, are configured by default to be members of VLAN 1. In a VLAN-based network, switches use VLAN1 as the default VLAN for in-band management and to communicate with other networking devices using Spanning-Tree Protocol (STP), Cisco Discovery Protocol (CDP), Dynamic Trunking Protocol (DTP), VLAN Trunking Protocol (VTP), and Port Aggregation Protocol (PAgP)all untagged traffic. As a consequence, VLAN 1 may unwisely span the entire network if not appropriately pruned. If its scope is large enough, the risk of compromise can increase significantly.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET SW VLAN1 In-Band MGT: If switch clustering is used, review the configuration of the VLAN command switch and look for the command cluster management-vlan. The new management VLAN ID follows this command.

For unclustered switches, review the configuration of each switch. All ports, including the internal management interface (sc0), are configured by default to be members of VLAN 1. The management VLAN can be identified by its switch virtual interface (SVI) defined that contains the IP address for the internal management interface. Note the IP address defined for the sc0 interface. The IP address of the sc0 interface can be accessed only by hosts connected to ports that belong to the management VLAN. Below is an example of disabling VLAN 1 and creating an SVI that could be used for the management VLAN.

interface VLAN1
no ip address
shutdown
interface VLAN10
ip address 10.0.1.10 255.255.255.0
no shutdown

Note: The management VLAN can also be defined by the set command when configuring the IP address of the Sc0.

set interface sc0 10.0.1.10 255.255.255.0

###Fixes###

NET SW VLAN1 In-Band MGT: Best practices for VLAN-based networks is create a dedicated management VLAN, prune unnecessary ports from gaining access to VLAN1 as well as the management VLAN, and to separate in-band management, device protocol, and data traffic.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1411 CAT: 2 The management VLAN is not secured.

Router Type:

Target(s): Layer 2 Switch; Layer 3 Switch

8500.2 IA Control: ECSC-1

Category: 14.5 - Physical Layer Security

Condition(s): Layer 2 Switch: Layer 3 Switch

Vulnerability The IAO/NSO will ensure the management VLAN is not configured on any trunk or access port that does not require it.

Vulnerability Discussion: All ports, including the internal sc0 interface, are configured by default to be members of VLAN 1. In a VLAN-based network, switches use VLAN1 as the default VLAN for in-band management and to communicate with other networking devices using Spanning-Tree Protocol (STP), Cisco Discovery Protocol (CDP), Dynamic Trunking Protocol (DTP), VLAN Trunking Protocol (VTP), and Port Aggregation Protocol (PAgP)all untagged traffic. As a consequence, VLAN 1 may unwisely span the entire network if not appropriately pruned. If its scope is large enough, the risk of compromise can increase significantly.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET SW Mgt VLAN restrict use: Review the switch configurations and note any ports assigned to the management VLAN. Only ports that should belong to the management VLAN are the trunk ports and the access ports of the switch administrator. It is possible that not all trunk ports need to belong to the management VLAN—trunk traffic is only required from the switches that have management workstations attached.

###Fixes###

NET SW Mgt VLAN restrict use: Best practices for VLAN-based networks is create a dedicated management VLAN, prune unnecessary ports from gaining access to VLAN1 as well as the management VLAN, and to separate in-band management, device protocol, and data traffic.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1412 CAT: 2 VLAN 1 is being used as a user VLAN.

Router Type:

Target(s): Layer 2 Switch; Layer 3 Switch

8500.2 IA Control:

Category: 14.5 - Physical Layer Security

Condition(s): Layer 2 Switch: Layer 3 Switch

Vulnerability The IAO/NSO will ensure VLAN1 is not used for user VLANs.

Vulnerability Discussion: In a VLAN-based network, switches use VLAN1 as the default VLAN for in-band management and to communicate with other networking devices using Spanning-Tree Protocol (STP), Cisco Discovery Protocol (CDP), Dynamic Trunking Protocol (DTP), VLAN Trunking Protocol (VTP), and Port Aggregation Protocol (PAgP)—all untagged traffic. As a consequence, VLAN 1 may unwisely span the entire network if not appropriately pruned. If its scope is large enough, the risk of compromise can increase significantly.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET SW VLAN1 Shutdown: Review the switch configurations and verify that no access ports have been assigned membership to the VLAN 1. A good method of ensuring there is not membership to VLAN 1 is to have the following configured:

interface VLAN1
no ip address
shutdown

This technique does not prevent switch control plane protocols such as CDP, DTP, VTP, and PAgP from using VLAN 1.

A show vlan 1 command can be used to verify what ports are assigned to VLAN 1.

###Fixes###

NET SW VLAN1 Shutdown: Best practices for VLAN-based networks is to prune unnecessary ports from gaining access to VLAN1 as well as the management VLAN, and to separate in-band management, device protocol, and data traffic.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1413 CAT: 3 VLAN 1 traffic traverses across unnecessary trunk

Router Type:

Target(s): Layer 2 Switch; Layer 3 Switch

8500.2 IA Control: ECSC-1

Category: 14.5 - Physical Layer Security

Condition(s): Layer 2 Switch: Layer 3 Switch

Vulnerability The IAO/NSO will ensure VLAN1 is pruned from all trunk and access ports that do not require it.

Vulnerability Discussion: VLAN 1 is a special VLAN that tags and handles most of the control plane traffic such as Spanning-Tree Protocol (STP), Cisco Discovery Protocol (CDP), Dynamic Trunking Protocol (DTP), VLAN Trunking Protocol (VTP), and Port Aggregation Protocol (PAgP)all VLAN 1 tagged traffic. VLAN 1 is enabled on all trunks and ports by default. With larger campus networks, care needs to be taken about the diameter of the VLAN 1 STP domain; instability in one part of the network could affect VLAN 1, thereby influencing control-plane stability and therefore STP stability for all other VLANs.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET SW VLAN1 Port Useage: Review the switch configurations and note any ports assigned to VLAN 1. A show vlan command can also be used to verify what ports are assigned to VLAN 1.

###Fixes###

NET SW VLAN1 Port Useage: Best practice for VLAN-based networks is to prune unnecessary ports from gaining access to VLAN1 and insure that it does not traverse trunks not requiring VLAN1 traffic.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1416 CAT: 2 Ensure trunking is disabled on all access ports.

Router Type:

Target(s): Layer 2 Switch; Layer 3 Switch

8500.2 IA Control: ECSC-1

Category: 14.5 - Physical Layer Security

Condition(s): Layer 2 Switch: Layer 3 Switch

Vulnerability The IAO/NSO will ensure trunking is disabled on all access ports (do not configure trunk on, desirable, non-negotiate, or auto—only off).

Vulnerability Discussion: Double encapsulation can be initiated by an attacker who has access to a switch port belonging to the native VLAN of the trunk port. Knowing the victims MAC address and with the victim attached to a different switch belonging to the same trunk group, thereby requiring the trunk link and frame tagging, the malicious user can begin the attack by sending frames with two sets of tags. The outer tag that will have the attackers VLAN ID (probably the well known and omnipresent VLAN1) is stripped off by the switch, and the inner tag that will have the victims VLAN ID is used by the switch as the next hop and sent out the trunk port.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET SW Trunking on Access Port: Review the switch configurations and examine all access ports. Verify that the port is not in trunk mode (i.e. for Catalyst using IOS the interface should have the command switchport mode access—not switchport mode trunk or older switches trunk off and not trunk on). A show trunk command can also be used to display all ports in trunk mode. Trace the connections from the physical port with trunk mode. This should be a Gigabit Ethernet or Fast Ethernet connection to another switch or router—it should not be connected to a workstation.

###Fixes###

NET SW Trunking on Access Port: Disable trunking on all access ports.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1417 CAT: 2 A dedicated VLAN is required for all trunk ports.

Router Type:

Target(s): Layer 2 Switch; Layer 3 Switch

8500.2 IA Control: ECSC-1

Category: 14.5 - Physical Layer Security

Condition(s): Layer 3 Switch: Layer 2 Switch

Vulnerability The IAO/NSO will ensure when trunking is necessary; a dedicated VLAN is configured for all trunk ports.

Vulnerability Discussion: Double encapsulation can be initiated by an attacker who has access to a switch port belonging to the native VLAN of the trunk port. Knowing the victims MAC address and with the victim attached to a different switch belonging to the same trunk group, thereby requiring the trunk link and frame tagging, the malicious user can begin the attack by sending frames with two sets of tags. The outer tag that will have the attackers VLAN ID (probably the well known and omnipresent VLAN1) is stripped off by the switch, and the inner tag that will have the victims VLAN ID is used by the switch as the next hop and sent out the trunk port.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET SW Trunk Dedicated VLAN : Review the switch configurations and examine all trunk ports. Verify that they belong to their own VLAN. Following is an example of assigning a trunk port to a VLAN:

```
interface FastEthernet0/23
description Trunk Port
no ip address
no cdp enable
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk native
vlan 55
no shutdown
```

A show vlan command can also be used to verify what VLAN the trunked ports are assigned to.

###Fixes###

NET SW Trunk Dedicated VLAN : To ensure the integrity of the trunk link and prevent unauthorized access, the native VLAN of the trunk port should be changed from the default VLAN1 to its own unique VLAN.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1418 CAT: 2 The VLAN is not configured to insure the integrity

Router Type:

Target(s): Layer 2 Switch; Layer 3 Switch

8500.2 IA Control: DCBP-1: ECSC-1: DCBP-1: ECSC-1

Category: 14.5 - Physical Layer Security

Condition(s): Layer 2 Switch: Layer 2 Switch: Layer 3 Switch: Layer 3 Switch

Vulnerability The IAO/NSO will ensure access ports are not assigned to the dedicated trunk VLAN.

Vulnerability Discussion: Double encapsulation can be initiated by an attacker who has access to a switch port belonging to the native VLAN of the trunk port. Knowing the victim's MAC address and with the victim attached to a different switch belonging to the same trunk group, thereby requiring the trunk link and frame tagging, the malicious user can begin the attack by sending frames with two sets of tags. The outer tag that will have the attacker's VLAN ID (probably the well known and omnipresent VLAN1) is stripped off by the switch, and the inner tag that will have the victim's VLAN ID is used by the switch as the next hop and sent out the trunk port.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET SW Access Port restriction: Review the switch configurations and examine all access ports. Verify that they do not belong to the trunk VLAN.

###Fixes###

NET SW Access Port restriction: To insure the integrity of the trunk link and prevent unauthorized access, the native VLAN of the trunk port should be changed from the default VLAN1 to its own unique VLAN.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1434 CAT: 2 Switch Access Control SRV using weak EAP protocol

Router Type:

Target(s): Layer 2 Switch; Layer 3 Switch

8500.2 IA Control: ECSC-1

Category: 14.5 - Physical Layer Security

Condition(s): Layer 2 Switch: Layer 3 Switch

Vulnerability The IAO/NSO will ensure when utilizing 802.1X, a secure EAP type(EAP-TLS, EAP-TTLS or PEAP) resides on the authentication sever and within the operating system or application software on the client devices.

Vulnerability Discussion: Lightweight EAP (LEAP) is a CISCO proprietary protocol providing an easy-to-deploy one password authentication. LEAP is vulnerable to dictionary attacks. A "man in the middle" can capture traffic, identify a password, and then use it to access a WLAN. LEAP is inappropriate and does not provide sufficient security for use on DOD networks.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET SW EAP Type not Secure (Manual) - Have the switch administrator identify the Access Control Server providing the authentication. Typically these have a GUI interface. Verify the server is not using a vulnerable EAP type as described in the STIG.

###Fixes###

NET SW EAP Type not Secure (Manual) - Have the switch administrator use a EAP type as described in the STIG.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1435 CAT: 3 Disabled ports are not kept in an unused VLAN.

Router Type:

Target(s): Layer 2 Switch; Layer 3 Switch

8500.2 IA Control: DCBP-1: ECSC-1: DCBP-1: ECSC-1

Category: 14.5 - Physical Layer Security

Condition(s): Layer 2 Switch: Layer 2 Switch: Layer 3 Switch: Layer 3 Switch

Vulnerability The IAO/NSO will ensure disabled ports are placed in an unused VLAN (do not use VLAN1).

Vulnerability Discussion: It is possible that a disabled port that is assigned to a user or management VLAN becomes enabled by accident or by an attacker and as a result gains access to that VLAN as a member.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET SW Disabled Ports : Review the switch configurations and examine all interfaces. Each interface not in use should have membership to a VLAN that is not used for any other purpose. Below would be an example.

interface FastEthernet0/5switchport
mode accessswitchport
access vlan 999shutdown

For older switches such as the Catalyst 1900, you would see something like the following:

interface FastEthernet0/5
vlan-membership static 999
shutdown

###Fixes###

NET SW Disabled Ports : Assign all disabled ports to an unused VLAN. Do not use VLAN1.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1436 CAT: 1 Port Security or 802.1x is not turned on.

Router Type:

Target(s): Layer 2 Switch; Layer 3 Switch

8500.2 IA Control: ECSC-1

Category: 14.5 - Physical Layer Security

Condition(s): Layer 2 Switch: Layer 3 Switch

Vulnerability The IAO/NSO will ensure either Port Security or 802.1X Port Authentication is used on all access ports.

Vulnerability Discussion: Eliminating unauthorized access to the network from inside the enclave is vital to keeping a network secure. Internal access to the private network is enabled by simply connecting a workstation or laptop to a wall plate or access point located in the work area.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET SW Port Security or 802.1x: Catalyst Procedure: Port Security: Have the switch administrator issue a show port [mod[/port]] or look for the following command. set port security 2/1 enable

IOS Procedure: 802.1x: Having the switch administrator issue a show port [mod[/port]] will also provide the detail.

```
aaa new-model
aaa authentication dot1x
default group radius
dot1x system-auth-control

interface fastethernet 5/1
dot1x port-control auto
```

###Fixes###

NET SW Port Security or 802.1x: Enable Port Security or 802.1x on all switch ports.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1437 CAT: 2 Port Security with MAC Addresses is not configured

Router Type:

Target(s): Layer 2 Switch; Layer 3 Switch

8500.2 IA Control: ECSC-1

Category: 14.5 - Physical Layer Security

Condition(s): Layer 2 Switch: Layer 3 Switch

Vulnerability The IAO/NSO will ensure if Port Security has been implemented, the MAC addresses are statically configured on all access ports.

Vulnerability Discussion: Eliminating unauthorized access to the network from inside the enclave is vital to keeping a network secure. Internal access to the private network is enabled by simply connecting a workstation or laptop to a wall plate or access point located in the work area.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET SW Port Secured MAC ADDR: Have the switch administrator issue a show port [mod[/port]] or look for the following command.

set port security mod/port enable MAC address

###Fixes###

NET SW Port Secured MAC ADDR: Enable Port Security with MAC Addresses.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1438 CAT: 3 All 802.1x access ports must start in the unauthor

Router Type:

Target(s): Layer 2 Switch; Layer 3 Switch

8500.2 IA Control: ECSC-1

Category: 14.5 - Physical Layer Security

Condition(s): Layer 2 Switch: Layer 3 Switch

Vulnerability The IAO/NSO will ensure if 802.1X Port Authentication is implemented, all access ports start in the unauthorized state.

Vulnerability Discussion: Eliminating unauthorized access to the network from inside the enclave is vital to keeping a network secure. Internal access to the private network is enabled by simply connecting a workstation or laptop to a wall plate or access point located in the work area.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET SW Port Unauth State: 802.1 Security: Have the switch administrator issue a show dot1x all or look for the following command.

dot1x port-control force-unauthorized

###Fixes###

NET SW Port Unauth State: Configure the 802.1x ports to come up with an unauthorized initial status.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1439 CAT: 2 Re-authentication must occur every 60 minutes.

Router Type:

Target(s): Layer 2 Switch; Layer 3 Switch

8500.2 IA Control: ECSC-1

Category: 14.5 - Physical Layer Security

Condition(s): Layer 2 Switch: Layer 3 Switch

Vulnerability The IAO/NSO will ensure if 802.1x Port Authentication is implemented, re-authentication must occur every 60 minutes.

Vulnerability Discussion: Eliminating unauthorized access to the network from inside the enclave is vital to keeping a network secure. Internal access to the private network is enabled by simply connecting a workstation or laptop to a wall plate or access point located in the work area.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET SW 802.1x Reauthenticate: 802.1 Security: Review the switch configuration for the following command.
dot1x re-authenticate [interface interface-id]

###Fixes###

NET SW 802.1x Reauthenticate: Ensure 802.1x reauthentication occurs every 60 minutes.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1440 CAT: 3 For End-User access, the use of clear text Telnet,

Router Type:

Target(s): Remote Access Server

8500.2 IA Control: ECSC-1

Category: 8.1 - Encrypted Data in Transit

Condition(s): Remote Access Server

Vulnerability The IAO/NSO will ensure that end user access is limited and the use of clear text Telnet, TN3270, and other terminal emulator TCP/IP sessions employ encryption to the fullest extent possible.

Vulnerability Discussion: A hacker can simply wait for authentication of the remote user and then take over or hijack the session and assume the identity of an authorized user. Once the hacker has breached the private network as an authorized mobile user, an attack against strategic network components can be launched.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET RAS Telnet: Interview the IAO/NSO to determine if the site is compliant with this requirement.

###Fixes###

NET RAS Telnet: Examine remote device configuration to verify use of encryption. If encryption or VPN is not used, examine site's policy remote access agreement that should include wording that discourages use of clear text Telnet, TN3270, and other terminal emulator TCP/IP sessions. The site should devise a plan to eliminate the use of clear text sessions and move to an encrypted form of communication.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1441 CAT: 1 A non-certified solution is being used for RAS.

Router Type:

Target(s): Remote Access Server

8500.2 IA Control: ECSC-1: ECSC-1

Category: 4.10 - RAS

Condition(s): Remote Access Server: Remote Access Server

Vulnerability The IAO/NSO will ensure that an NSA Certified remote access security solution is in place for remote access to a classified network and is only used from an approved location.

- The solution will be used in accordance with all NSA and DOD policy and guidelines.
- The secure solution will support Key Exchange Algorithm (KEA).
- The secure solution will support Palladium Fortezza Modems.
- Each modem will have a valid X.509 V1 Certificate issued.
- The Fortezza card will be kept in the user's possession at all times or stored in accordance with policy applicable to classified storage.
- The modem will be stored separately from the computer when not in use.

Vulnerability Discussion: NSA, DISA, and the DOD have stringent policy on the access, storage, location, and containment of all classified data and processing. It is imperative that a secured solution is implemented prior to providing remote access to a classified network.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET RAS NSA Solution Deployed: Review the remote access security solution with the ISSO to determine if the site is compliant with this requirement.

###Fixes###

NET RAS NSA Solution Deployed: Prior to providing remote access to a classified network, insure that a secured solution is in place to insure the integrity, protection, and privacy of all classified data

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1446 CAT: 2 The remote access agreement is not IAW Policy.

Router Type:

Target(s): Remote Access Server

8500.2 IA Control: ECSC-1

Category: 12.4 - CM Process

Condition(s): Remote Access Server

Vulnerability The IAM will develop a policy for secure remote access to the site and an agreement between the site and remote user, to include, but not limited to, the following:

- The signed agreement will contain the type of access required by the user.

- The signed agreement will contain the responsibilities, liabilities, and security measures (e.g., malicious code detection training) involved in the use of their remote access device.

- Incident handling and reporting procedures will be identified along with a designated point of contact.

- The remote user can be held responsible for damage caused to a Government system or data through negligence or a willful act.

- The policy will contain general security requirements and practices and will be acknowledged and signed by the remote user.

- If classified devices are used for remote access from an alternative work site, the remote user will adhere to DOD policy in regard to facility clearances, protection, storage, distributing, etc.

- Government owned hardware and software will be used for official duties only. The employee is the only individual authorized to use this equipment.

Vulnerability Discussion: Without a formal personnel approval process and policy in place, unauthorized users may gain access to critical DOD systems. It is imperative that only the required access to the required systems and information be provided to each individual. Without control of the physical security at a DOD site that restricts personnel to their authorized areas any person may gain access to systems or network devices that could compromise those systems or networks and possibly other extended systems and networks.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET RAS User Agreement: Have the ISSO provide a copy of the policy and agreement for review.

###Fixes###

NET RAS User Agreement: The IAO will develop a policy for secure remote access and an agreement between the site and remote users.

The agreement will brief all users on the responsibilities, liabilities and security measures involved in the use of their PCs.

The agreement will identify incident handling, reporting procedures, and a point of contact.

The agreement will advise the user that they can be held responsible for damage caused to a Government system or data through negligence or a willful act.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1451 CAT: 2 RAS must use Two-factor authentication.

Router Type:

Target(s): Remote Access Server

8500.2 IA Control: EBRU-1: ECSC-1

Category: 12.4 - CM Process

Condition(s): Remote Access Server

Vulnerability The IAO/NSO will ensure that all remote users are required to use a form of two-factor authentication to access the network.

Vulnerability Discussion: Without strong two-factor authorization, unauthorized users may gain access to network managed devices such as routers or communications servers (CSs), etc. If the router network is compromised, large parts of the network could be incapacitated with only a few commands. If a CS is compromised, unauthorized users could gain access to the network and its attached systems. They could also disable the CS, keeping authorized subscribers from supporting mission critical functions.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET RAS Two-factor: Review the configuration of the authentication server.

###Fixes###

NET RAS Two-factor: The site will develop a secure remote access method to the network/end system.

Strong two-factor authentication will be employed.

All communication to/from the remote users will employ at a minimum a FIPS-140-2 approved encryption algorithm (e.g. 3DES).

The network administrator will adhere to Virtual Private Networks (VPNs,), if VPN technology is employed.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1452 CAT: 3 The remote access server does not log the required

Router Type:

Target(s): Remote Access Server

8500.2 IA Control: DCBP-1: ECSC-1: DCBP-1: ECSC-1

Category: 10.2 - Content Configuration

Condition(s): Remote Access Server: Remote Access Server

Vulnerability The IAO/NSO will ensure that the remote access infrastructure (i.e., authentication server, RAS/NAS device, VPN gateway) logs session connectivity and termination, userid, assigned IP address, and success or failure of all session events.

Vulnerability Discussion: Without the proper log information of all sessions, the NSO will have no method by which to investigate a possible breach of the network via remote access.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET RAS Session Logging: Review the configuration of the RAS/NAS and the authentication server.

###Fixes###

NET RAS Session Logging: Ensure that the authentication server and remote access server log the required session information.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1453 CAT: 3 RAS session session exceeds 30 min inactivity.

Router Type:

Target(s): Remote Access Server

8500.2 IA Control: ECSC-1: ECSC-1

Category: 4.10 - RAS

Condition(s): Remote Access Server: Remote Access Server

Vulnerability The IAO/NSO will ensure that a session that exceeds 30 minutes of inactivity is disconnected.

Vulnerability Discussion: An unattended remote connection to the network increases the risk of session hijacking.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET RAS Session Expiration: Review the configuration of the RAS/NAS.

###Fixes###

NET RAS Session Expiration: Ensure that the RAS/NAS device will terminate an inactive session.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1455 CAT: 3 The remote access logs are not retained online for

Router Type:

Target(s): Remote Access Server

8500.2 IA Control: ECRR-1: ECSC-1

Category: 10.5 - Retention

Condition(s): Remote Access Server

Vulnerability The IAO/NSO will ensure that the audit logs for any remote access server authentication mechanism are maintained for no less than a period of 30 days on line, and one year off-line.

Vulnerability Discussion: Logging is a critical part of system security. Maintaining an audit trail of activity via logs can help identify attempts to breach the network.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET RAS Log Retentioin: Review the configuration of the RAS/NAS.

###Fixes###

NET RAS Log Retention: Archive log data on the firewall for 30 days and keep offline for a minimum of one year.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1456 CAT: 3 The logs are not viewed on a weekly basis.

Router Type:

Target(s): Remote Access Server

8500.2 IA Control: ECAT-1: ECAT-2: ECSC-1

Category: 10.3 - Review

Condition(s): Remote Access Server

Vulnerability The IAO/NSO will ensure that the audit logs are viewed on a weekly basis.

Vulnerability Discussion: Logging is a critical part of system security. Maintaining an audit trail of activity via logs can help identify attempts to breach the network.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET RAS Log Reviews: Review site policy and interview IAO/NSO to determine compliance.

###Fixes###

The NSO will ensure that log d: The NSO will ensure that log data from remote access sessions or logon attempts are reviewed daily

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1460 CAT: 3 Modems are not physically protected.

Router Type:

Target(s): Remote Access Server

8500.2 IA Control: ECSC-1: PEPF-1: PEPF-2

Category: 4.10 - RAS

Condition(s): Remote Access Server

Vulnerability The IAO/NSO will ensure all modems are physically protected.

Vulnerability Discussion: Limiting the access to infrastructure modems and keeping accurate records of the deployed modems will limit the chance that unauthorized modems will be placed into the infrastructure. If an unauthorized person has physical access to a sites modems, the switch or software settings can be changed to affect the security of a system.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET RAS Modem Location: Visually inspect location of modems to determine compliance.

###Fixes###

NET RAS Modem Location: Ensure that all modems are physically protected.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1462 CAT: 4 Maintaining an accurate list of all modems.

Router Type:

Target(s): Remote Access Server

8500.2 IA Control: ECSC-1

Category: 12.9 - Documentation

Condition(s): Remote Access Server

Vulnerability The IAO/NSO will maintain a listing of all modems, associated phone number, and location.

Vulnerability Discussion: Keeping accurate records of the deployed modems will limit the chance that unauthorized modems will be placed into the infrastructure.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET RAS Modem List: Have the IAO/NSO provide the list for visual inspection.

###Fixes###

NET RAS Modem List: Ensure an accurate listing of all infrastructure modems is maintained IAW the Network Infrastructure STIG.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1470 CAT: 3 Modems are not restricted to single-line and singl

Router Type:

Target(s): Remote Access Server

8500.2 IA Control: ECSC-1

Category: 4.10 - RAS

Condition(s): Remote Access Server

Vulnerability The IAO/NSO will ensure that all modem phone lines are restricted to single-line operation if dial back services are not used (inward dial only or outward dial only) without any special features (e.g., call forwarding).

Vulnerability Discussion: Ubiquitous phone lines open major security holes in a network. The more tightly they can be controlled, the less the exposure to vulnerabilities. Allowing special features to remain active on modem phone lines create advantageous situations for malicious attacks. An attacker may use special features to forward modem or voice calls to destinations that cause toll-fraud, or forward the number to itself causing a denial of service.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET RAS Lines Single Operation: Interview the Network Administrator.

###Fixes###

NET RAS Lines Single Operation: The NSO will ensure that all modem lines are restricted to single line operation and configured to their mission required purpose (inward or outward dial only), without any special features (i.e call forwarding).

The NSO will ensure that if the modems use is infrequent and relatively predictable, the line will be disconnected until needed.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1530 CAT: 3 Proper Caller ID logs are not being maintained.

Router Type:

Target(s): Remote Access Server

8500.2 IA Control: ECSC-1

Category: 10.5 - Retention

Condition(s): Remote Access Server

Vulnerability The IAO/NSO will maintain ANI logs to provide a call audit trail.

Vulnerability Discussion: Ubiquitous phone lines open major security holes in a network. The more tightly they can be controlled, the less the exposure to vulnerabilities. Allowing special features to remain active on modem phone lines create advantageous situations for malicious attacks. An attacker may use special features to forward modem or voice calls to destinations that cause toll-fraud, or forward the number to itself causing a denial of service. ANI logs are ideal for auditing unauthorized accesses and toll-fraud.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET RAS ANI Logs: Interview the IAO and ask to see a copy of the logs.

###Fixes###

NET RAS ANI Logs: Maintain and review ANI logs. Audit records should be stored for a period of twelve months.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1535 CAT: 3 Callback procedures are not configured correctly.

Router Type:

Target(s): Remote Access Server

8500.2 IA Control: ECSC-1

Category: 12.9 - Documentation

Condition(s): Remote Access Server

Vulnerability The Network Administrator (NA) will ensure that if callback procedures are used, upon establishment of the callback connection, the communications device requires the user to authenticate to the system.

Vulnerability Discussion: Callback features are an attempt to protect the network by providing a service that disconnects an incoming call and reestablishes the call, dialing back to a predetermined number. Upon establishment of the callback connection, the communications device will require the user to authenticate to the system.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET RAS Callback Autheneticate: Have the IAO/NSO demonstrate the functionality.

###Fixes###

NET RAS Callback Autheneticat: The NSO will ensure that if Callback procedures are used, then upon establishment of the callback connection, the communications device will require the user to authenticate to the system.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1595 CAT: 2 RAS/NAS server is not located in a screened subnet

Router Type:

Target(s): Remote Access Server

8500.2 IA Control: EBRU-1: ECSC-1

Category: 4.10 - RAS

Condition(s): Remote Access Server

Vulnerability The IAO/NSO will ensure that the RAS/NAS device is located in a DMZ or screened subnet, thereby providing protection to the server while enforcing remote user access under the same remote access policy as those connecting by VPN.

Vulnerability Discussion: Allowing a remote connection to the private network unchecked by the firewall enables a mobile user to violate the security policy and put the network infrastructure in a vulnerable position. The risk would be magnified if a remote access session were hijacked.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET RAS Location: Review the network topology diagram. Check the RAS/NAS IP address and subnet mask to validate that it is in the documented subnet for the DMZ or screened subnet.

###Fixes###

NET RAS Location: Ensure that the RAS/NAS device is located in a DMZ or screened subnet, thereby providing protection to the server while enforcing remote user access under the same remote access policy as those connecting by VPN.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1600 CAT: 2 Use of in-band management is not limited.

Router Type:

Target(s): Remote Access Server

8500.2 IA Control: ECSC-1

Category: 4.7 - Routers

Condition(s): Remote Access Server

Vulnerability The IAO/NSO will limit the use of in-band management to situations where the use of OOB management would hinder operational commitments or when emergency situations arise. The IAO/NSO will approve the use of in-band management on a case-by-case documented basis.

Vulnerability Discussion: It is imperative that communications used for administrative access to a remote access server is limited to emergency situations or where out-of-band management would hinder daily operational requirements. In-band management introduces the risk of an attacker gaining access to the server internally or even externally.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET RAS In-band Mgt Limited: Interview the IAO/NSO for compliance.

###Fixes###

NET RAS In-band Mgt Limited: Use out-of-band management.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1602 CAT: 2 Two-factor authentication is not used for in-band

Router Type:

Target(s): Remote Access Server

8500.2 IA Control: ECSC-1: IAAC-1: IAIA-1: IAIA-2

Category: 1.4 - Authentication Services

Condition(s): Remote Access Server

Vulnerability The IAO/NSO will ensure for in-band management, that the site implements the use of strong two-factor authentication.

Vulnerability Discussion: Without strong two-factor authorization, unauthorized users may gain access to the access server that could lead to the entire network being compromised.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET RAS In-band Two-factor: Interview the IAO/NSO have an administrator establish a management session to determine compliance.

###Fixes###

NET RAS In-band Two-factor: Two factor authentication required for In-band Mgt sessions.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1604 CAT: 2 In-band management is not restricted to a limited

Router Type:

Target(s): Remote Access Server

8500.2 IA Control: ECND-1: ECND-2: ECSC-1

Category: 4.7 - Routers

Condition(s): Remote Access Server

Vulnerability The IAO/NSO will ensure that the use of in-band management is restricted to a limited number of authorized IP addresses. The number of IP addresses must be equal or less than the number of network engineers.

Vulnerability Discussion: Without limited in-band management connections, unauthorized users may gain access to the server and could then compromise the entire network.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET RAS Inband-Limited: Examine the access server configuration to determine what IP addresses are permitted access. If a terminal server is being used to access network equipment, this will need to be examined as well.

###Fixes###

Net Ras In-band Limited: For in-band management, the administrator will configure the network device to restrict the use of in-band connections to a limited number (less than 10) of authorized IP addresses.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1606 CAT: 2 In-band management access to a remote access serve

Router Type:

Target(s): Remote Access Server

8500.2 IA Control: ECNK-1: ECSC-1

Category: 8.1 - Encrypted Data in Transit

Condition(s): Remote Access Server

Vulnerability The IAO/NSO will ensure that all in-band management access to all remote access servers are secured using FIPS 140-2 validated encryption such as AES, 3DES, SSH, or SSL.

Vulnerability Discussion: Without encrypted in-band management connections, unauthorized users may gain control of a remote access server. If any remote access server is breached, the entire network could be compromised.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET RAS FIPS 140-2 required: Examine all remote access server configurations to verify that only SSH connections are permitted access.

###Fixes###

NET RAS FIPS 140-2 required: For in-band management the remote access server will configure the firewall to only allow SSH connections.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1610 CAT: 2 The Network Access Server (NAS) is not configured

Router Type:

Target(s): Remote Access Server

8500.2 IA Control: EBRU-1: ECSC-1

Category: 4.10 - RAS

Condition(s): Remote Access Server

Vulnerability The IAO/NSO will ensure that all remote clients and remote access servers are configured to use PPP instead of SLIP to provide the dial-up communication link.

The IAO/NSO will ensure that CHAP with MD5 or MS-CHAP with MD4 encryption is used to authenticate the remote client.

Vulnerability Discussion: To securely protect the network, Network Access Servers (NAS) and access to them must be controlled to guard against outside or unauthorized intrusion, which could result in system or network compromise. If the NAS is accessed remotely, the risk of compromising a password or userID increases. The authentication of the remote nodes must be controlled by encryption such as CHAP with MD5 or MS-CHAP with MD4.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET RAS PPP: Review the configuration for the RAS/NAS

###Fixes###

NET RAS PPP: The NSO will ensure the NAS is configured to accept only PPP connections.

The NSO will ensure that an accepted method of encryption to authenticate the remote node is used. (e.g. CHAP with MD5 or MS-CHAP with MD4).

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1625 CAT: 2 VPN gateway is located behind the firewall.

Router Type:

Target(s): VPN

8500.2 IA Control: EBVC-1: ECSC-1

Category: 4.2 - VPN

Condition(s): VPN

Vulnerability The IAO/NSO will ensure that VPN gateways terminate on or outside of the firewall.

Vulnerability Discussion: Allowing a remote connection to the private network unchecked by the firewall enables a mobile user to violate the security policy and put the network infrastructure in a vulnerable position. The risk would be magnified if the VPN connection were hijacked.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET VPN Termination: Review the network topology diagram and examine firewall rules to verify that there are no encrypted tunnels (i.e. IPSec) passing through the firewall.

###Fixes###

NET VPN Termination: Ensure that all VPN gateways terminate at or outside the firewall (e.g., between the premise router and the firewall, or connected to an outside interface of the router).

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1630 CAT: 2 The VPN connection is not using IPSec's ESP tunnel

Router Type:

Target(s): VPN

8500.2 IA Control: ECSC-1

Category: 4.2 - VPN

Condition(s): VPN

Vulnerability The IAO/NSO will ensure that remote access via VPN uses IPSec ESP in tunnel mode. For legacy support, L2TP may be used if IPSec provides encryption (DAA approval required), or another technology that secures using FIPS 140-2 validated encryption such as AES, 3DES, SSH, or SSL.

Vulnerability Discussion: AH (Authentication Header) mode only provides integrity protection by authentication each packet. However, the headers and data are not encrypted. In transport mode, IPSec encrypts only the data component of the IP packet to be transported: application headers, TCP/UDP headers and data are encrypted, the original IP headers are readable exposing the client's source address.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET VPN IPSEC ESP: Interview the NSO, review the network topology diagram, and review VPN concentrators.

###Fixes###

NET VPN IPSEC ESP: Ensure that remote access via VPN will use IPSec ESP in tunnel mode.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1650 CAT: 2 IPSEC is not being used to secure traffic being se

Router Type:

Target(s): Network/Element Management Server

8500.2 IA Control: ECSC-1

Category: 8.1 - Encrypted Data in Transit

Condition(s): Network/Element Management Server

Vulnerability The IAO/NSO will ensure IPSec is used to secure traffic between the network management workstation on DOD-managed LANs and all monitored devices sent via the Internet, NIPRNet, SIPRNet, or other external network.

Vulnerability Discussion: To securely protect the network, Network Management Systems (NMS) and access to them must be controlled to guard against outside or unauthorized intrusion, which could result in system or network compromise. Allowing any device to send traps or information may create a false positive and having site personnel perform unneeded or potentially hazardous actions on the network in response to these false traps. These sessions must be controlled and secured by IPSec.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET SNMP IPSEC: Interview the network administrator to ensure that IPSEC is being used to secure traffic sent between network management center workstations and all monitored devices.

###Fixes###

NET SNMP IPSEC: The NSO will ensure IPSec is used to secure traffic sent between network management workstations and all monitored devices.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1660 CAT: 1 An insecure version of SNMP is being used.

Router Type:

Target(s): Router

8500.2 IA Control: ECSC-1

Category: 4.7 - Routers

Condition(s): Router

Vulnerability The IAO/NSO will ensure that the SNMP Version 3 Security Model (both MD5 packet authentication and DES encryption of the PDU) is used across the entire network infrastructure.

NOTE: If the site is using Version 1 or Version 2 with all of the appropriate patches to mitigate the known security vulnerabilities, this finding can be downgraded to a Category II. If the site is using Version 1 or Version 2 with all of the appropriate patches and has developed a migration plan to implement the Version 3 Security Model, this finding can be downgraded to a Category III.

Vulnerability Discussion: SNMP Versions 1 and 2 are not considered secure. Without the strong authentication and privacy that is provided by the SNMP Version 3 User-based Security Model (USM), an attacker or other unauthorized user may gain access to detailed network management information and use that information to launch attacks against the network.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET SNMP Version: Interview the network administrators and examine configurations of managed nodes (routers, switches, etc).

###Fixes###

NET SNMP Version: The NSO will ensure that the SNMP Version 3 Security Model (both MD5 packet authentication and DES encryption of the PDU) will be used across the entire network infrastructure.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1665 CAT: 1 System community names or usernames use defaults

Router Type:

Target(s): Router

8500.2 IA Control: ECSC-1: IAIA-1: IAIA-2

Category: 1.3 - Identity Management

Condition(s): Router

Vulnerability The IAO/NSO will ensure that all SNMP community strings are changed from the default values.

Vulnerability Discussion: Community strings default to the name PUBLIC. This is known by those wishing to exert an attack against the devices in the network. This must be changed to something that is in compliance with DISA password guidelines. Not all individuals need write access to the device. Compromising the read password will have less of an impact if it cannot be used to change information. An erroneous message being sent to the NMS can cause network managers to act inappropriately in responding to an alarm or warning. It is important that the information being received is from valid managed devices.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET SNMP Community Strings: Interview the network administrators and examine configurations of managed nodes (routers, switches, etc).

###Fixes###

NET SNMP Community Strings: Most network management systems (NMSs) default to a community sign on name of public. This community name will be changed to something that is not easily guessed. It will be protected in the same way as any password is protected.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1666 CAT: 2 System community names, usernames, or passwords do

Router Type:

Target(s): Network/Element Management Server

8500.2 IA Control: ECSC-1

Category: 1.1 - Passwords

Condition(s): Network/Element Management Server

Vulnerability The IAO/NSO will ensure that all SNMP community strings and usernames are protected via technology that secures using FIPS 140-2 validated encryption such as AES, 3DES, SSH, or SSL.

Vulnerability Discussion: Compromising the network can cause erroneous messages being sent to the NMS that can cause network managers to act inappropriately in responding to an alarm or warning. It is important that the information being received is from valid managed devices.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET SNMP FIPS 140-2: Interview the network administrators and examine configurations of managed nodes (routers, switches, etc).

###Fixes###

NET SNMP FIPS 140-2: Network management systems (NMSs) will be protected in the same way as any password is protected via FIPS 140-2 approved data encryption.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1670 CAT: 3 An SNMP Standard Operating Procedure (SOP) is not

Router Type:

Target(s): Network/Element Management Server

8500.2 IA Control: ECSC-1: IAIA-1: IAIA-2

Category: 1.6 - Documentation and Storage

Condition(s): Network/Element Management Server

Vulnerability The IAO/NSO will establish and maintain a standard operating procedure managing SNMP community strings and usernames to include the following:

- Community string and username expiration period
- SNMP community string and username distribution including determination of membership

Vulnerability Discussion: Without a SOP to manage the SNMP community strings, the chance that these strings will be used to gain access to network managed devices is increased. If an attacker gains access to network devices, denial of service, interception of sensitive information, or other destructive actions could take place.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET SNMP SOP: Interview the IAO/NSO to ensure a documented SOP is in place for the management of SNMP community strings and usernames.

###Fixes###

NET SNMP SOP: The NSO will ensure that procedures are included in the documented SOP for the network to manage SNMP community strings. At a minimum, these procedures will include SNMP string expiration, SNMP string compromise, and SNMP string creation.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1675 CAT: 2 Exclusive use of privileged and non-privileged

Router Type:

Target(s): Router

8500.2 IA Control: ECSC-1

Category: 2.2 - Least Privilege

Condition(s): Router

Vulnerability The IAO/NSO will ensure that if both privileged and non-privileged modes are used on all devices. Different community names will be used for read-only access and read-write access.

Vulnerability Discussion: Numerous vulnerabilities exist with SNMP, therefore, without unique SNMP community names, the risk of compromise is dramatically increased. This is especially true with vendors default community names which are widely known by hackers and other networking experts. If a hacker gains access to these devices and can easily guess the name, this could result in denial of service, interception of sensitive information, or other destructive actions.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET SNMP Least Privilege: Review the configuration of all managed nodes (SNMP agents) to ensure that different community names or usernames are used for read-only and read-write access.

###Fixes###

NET SNMP Least Privilege: The NSO will ensure that SNMP community names are changed from the default public values to unique community names and developed IAW the Network Infrastructure STIG.

The NSO will ensure these names do not match any other network device passwords, keys or strings.

The NSO will ensure that unique community names are used for different access types, including read-only, read and write.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1710 CAT: 3 Proper categories of security violations are not p

Router Type:

Target(s): Network/Element Management Server

8500.2 IA Control: ECSC-1

Category: 10.4 - Reporting

Condition(s): Network/Element Management Server

Vulnerability The IAO/NSO will ensure that security alarms are set up within the managed network's framework. At a minimum, these will include the following:

- Integrity Violation: Indicates that network contents or objects have been illegally modified, deleted, or added.

- Operational Violation: Indicates that a desired object or service could not be used.

- Physical Violation: Indicates that a physical part of the network (such as a cable) has been damaged or modified without authorization.

- Security Mechanism Violation: Indicates that the network's security system has been compromised or breached.

- Time Domain Violation: Indicates that an event has happened outside its allowed or typical time slot.

Vulnerability Discussion: Without the proper categories of security alarms being defined on the NMS, responding to critical outages or attacks on the network may not be coordinated correctly with the right personnel, hardware, software or vendor maintenance. Delays will inevitably occur which will cause network outages to last longer than necessary or expose the network to larger, more extensive attacks or outages.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET SNMP Security Alarms: Request that the network engineer demonstrate the alert capabilities.

###Fixes###

NET SNMP Security Alarms: The NSO will ensure that the NMS is configured, at a minimum, to alarm on the following security violations: integrity, operational, physical, security mechanism, and time domain violation.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1720 CAT: 3 NMS security alarm severity levels are not categor

Router Type:

Target(s): Network/Element Management Server

8500.2 IA Control: ECSC-1

Category: 10.4 - Reporting

Condition(s): Network/Element Management Server

Vulnerability The IAO/NSO will ensure that alarms are categorized by severity using the following guidelines:

- Critical and major alarms are given when a condition that affects service has arisen. For a critical alarm, steps must be taken immediately in order to restore the service that has been lost completely.

- A major alarm indicates that steps must be taken as soon as possible because the affected service has degraded drastically and is in danger of being lost completely.

- A minor alarm indicates a problem that does not yet affect service, but may do so if the problem is not corrected.

- A warning alarm is used to signal a potential problem that may affect service.

- An indeterminate alarm is one that requires human intervention to decide its severity.

Vulnerability Discussion: Without the proper categories of severity levels being defined on the NMS, outages or attacks may not be responded to by order of criticality. If a critical attack or outage is not responded to first, then there will be a delay in fixing the problem, which may cause network outages to last longer than necessary or expose the network to larger more extensive attacks or outages.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET SNMP Alarm Categories: Request that the network engineer demonstrate the alert capabilities.

###Fixes###

NET SNMP Alarm Categories: The NSO will ensure that the NMS security alarm severity levels are configured as critical, major, minor, warning and indeterminate.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1730 CAT: 2 The NMS is not located in a secure environment.

Router Type:

Target(s): Network/Element Management Server

8500.2 IA Control: ECSC-1: PEPF-1: PEPF-2

Category: 5.9 - Device Locations

Condition(s): Network/Element Management Server

Vulnerability The IAO/NSO will ensure that the management workstation is located in a secure environment.

Vulnerability Discussion: Many attacks on DOD computer systems are launched from within the network by unsatisfied or disgruntled employees, therefore, it is imperative that the NMS be located in a secure area that allows access to authorized personnel only. If unauthorized users gain access to the NMS, they could change device configurations, cause network disruptions, or create denial of service conditions.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET NMS Location: Inspect the location of the network management workstations.

###Fixes###

NET NMS Location: The NOC will ensure that the NMS is located in a secure environment approved for at least secret level processing.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1740 CAT: 2 NMS accounts are not properly maintained.

Router Type:

Target(s): Network/Element Management Server

8500.2 IA Control: ECSC-1: IAAC-1

Category: 1.3 - Identity Management

Condition(s): Network/Element Management Server

Vulnerability The IAO/NSO will ensure that only those accounts necessary for the operation of the system and for access logging are maintained.

Vulnerability Discussion: Without proper account maintenance, unauthorized users could gain access to the NMS. If unauthorized users gain access to the NMS through an invalid account they could change device configurations or cause denial of service conditions.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET NMS Accounts: Review the configuration of the NMS with the IAO/NSO to verify that proper account administration is being enforced. Review the accounts and the personnel using them to verify that they require access.

###Fixes###

NET NMS Accounts: The NSO will ensure that procedures are in place to enforce proper account administration. The NSO will ensure that any account that is no longer needed will be disabled or removed from the system.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1750 CAT: 3 Logons and transactions are not being recorded.

Router Type:

Target(s): Network/Element Management Server

8500.2 IA Control: ECAR-1: ECAR-2: ECAR-3: ECSC-1

Category: 10.2 - Content Configuration

Condition(s): Network/Element Management Server

Vulnerability The IAO/NSO will ensure a record is maintained of all logons and transactions processed by the management station.

NOTE: Include time logged in and out, devices that were accessed and modified, and other activities performed.

Vulnerability Discussion: Logging is a critical part of network security. Maintaining an audit trail of system activity logs can help identify configuration errors, understand past intrusions, troubleshoot service disruptions, and react to probes and scans of the network. Audit logs are also necessary to provide a trail of evidence in case the network is compromised. Without an audit trail that provides a when, where, who and how set of information, repeat offenders could continue attacks against the network indefinitely. With this information, the network administrator can devise ways to block the attack and possibly identify and prosecute the attacker.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET NMS Logs: Review the NMS configuration and logs

###Fixes###

NET NMS Logs: The NSO will ensure that the NMS records all logons and transactions on the management station. The log will include at a minimum: time logged in and out, devices that were accessed and modified, and other activities performed. The audit will be stored online for a minimum of 30 days and offline for at least one year.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1760 CAT: 1 Logon access to the NMS is not restricted.

Router Type:

Target(s): Network/Element Management Server

8500.2 IA Control: ECSC-1: IAIA-1: IAIA-2

Category: 1.3 - Identity Management

Condition(s): Network/Element Management Server

Vulnerability The IAO/NSO will ensure access to the NMS is restricted to authorized users with individual userids and passwords.

Vulnerability Discussion: If unauthorized users gain access to the NMS they could change device configurations and SNMP variables that can cause disruptions and even denial of service conditions.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET NMS Identity Management: Review the NMS configuration to verify compliancy.

###Fixes###

NET NMS Identity Management: The NOC will ensure that access to the NMS is available only to authorized users with appropriate userids and passwords.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1762 CAT: 2 In-band access to the NMS is not encrypted.

Router Type:

Target(s): Network/Element Management Server

8500.2 IA Control: ECNK-1: ECSC-1

Category: 8.1 - Encrypted Data in Transit

Condition(s): Network/Element Management Server

Vulnerability The IAO/NSO will ensure that all in-band sessions to the NMS is secured using FIPS 140-2 validated encryption such as AES, 3DES, SSH, or SSL.

Vulnerability Discussion: Without encrypted in-band management connections, unauthorized users may gain access to the NMS enabling them to change device configurations and SNMP variables that can cause disruptions and even denial of service conditions.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET NMS In-band FIPS 140-2: Review the configuraton for the NMS to verify that only SSH can be used to access the NMS.

###Fixes###

NET NMS In-band FIPS 140-2: For in-band management, the router administrator will configure the network device to only allow SSH connections.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1770 CAT: 2 Access to the NMS is not restricted by IP address.

Router Type:

Target(s): Network/Element Management Server

8500.2 IA Control: ECSC-1

Category: 2.2 - Least Privilege

Condition(s): Network/Element Management Server

Vulnerability The IAO/NSO will ensure connections to the NMS are restricted by IP address to only the authorized devices being monitored..

Vulnerability Discussion: Without restricting device connections by IP address to the NMS, unauthorized devices or users could send bogus messages that might flood the system with invalid information , degrade its operation, or make it unusable.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET NMS Restricted LAN: Review the NMS configuration to verify compliancy.

###Fixes###

NET NMS Restricted LAN: The NSO will ensure that the access to the NMS is restricted by IP address to only the authorized devices being monitored.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1780 CAT: 2 The NMS password policy is not IAW the Network Inf

Router Type:

Target(s): Network/Element Management Server

8500.2 IA Control: ECSC-1

Category: 2.2 - Least Privilege

Condition(s): Network/Element Management Server

Vulnerability The IAO/NSO will ensure all accounts are assigned the lowest possible level of access/rights necessary to perform their jobs.

Vulnerability Discussion: Without a formal personnel approval process, unauthorized users may gain access to critical DoD systems. It is imperitive that only the required access to the required systems and information be provided to each individual.

The lack of a password protection for communications devices provides anyone access to the device, which opens a backdoor opportunity for intruders to attack and manipulate or compromise network resources. Vendors often assign default passwords to communication devices. These default passwords are well known to the hacker community and are extremely dangerous if left unchanged.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET NMS Least Privilege: Review the user database to determine compliance.

###Fixes###

NET NMS Least Privilege: Have the NSO ensure that accounts are created with the lowest privilege necessary to perform their duties.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1800 CAT: 2 VPN is not configured as a tunnel type VPN.

Router Type:

Target(s): VPN

8500.2 IA Control: EBVC-1: ECSC-1

Category: 4.2 - VPN

Condition(s): VPN

Vulnerability The IAO/NSO will ensure VPNs are established as tunnel type VPNs, which terminate outside the firewall (e.g., between the router and the firewall, or connected to an outside interface of the router).

Vulnerability Discussion: VPNs improperly deployed take away a firewalls ability to audit useful information, or to make decisions beyond the level of who is allowed to talk to whom. There are ways around this. The easiest way is for a hacker to make the firewall a trusted third member of the conversation.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET VPN Tunnel Type: Review the vendor documentation, then interview the NSO. Have the SA display the configuration settings that enable this feature.

###Fixes###

NET VPN Tunnel Type: Establish the VPN as a tunneled VPN.

Terminate the tunneled VPN outside of the firewall.

Ensure all host-to-host VPN are established between trusted known hosts.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1810 CAT: 3 Site has not maintained oversight of enclave.

Router Type:

Target(s): VPN

8500.2 IA Control: ECSC-1

Category: 4.2 - VPN

Condition(s): VPN

Vulnerability The IAM will ensure that the site retains administrative oversight and control privileges on the IPSEC/VPN device within their security enclave if access is granted to the local network.

Vulnerability Discussion: Without administrative oversight and control privileges on the VPN device, the site would have no way of verifying the security controls placed on the device.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET VPN Enclave Oversight: Interview the IAM to determine compliancy.

###Fixes###

NET VPN Enclave Oversight: When an agreement to establish a VPN with an outside security enclave/domain, retain administrative oversight and control privileges in the IPSEC/VPN device that is within your security enclave.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1820 CAT: 2 IDS does not monitor all the VPN traffic.

Router Type:

Target(s): VPN

8500.2 IA Control: EBVC-1: ECSC-1

Category: 4.5 - IDS

Condition(s): VPN

Vulnerability The IAM will require the customer to provide an Intrusion Detection System (IDS) capability (host IDS) for any VPN established that bypasses the site's current IDS capability.

Vulnerability Discussion: When the site enters into an agreement to allow a connection to bypass the sites IDS capability, the site needs to have a mechanism for detecting attacks or anomalies that transverse that connection.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET VPN IDS: Review the network topology diagram to determine compliance.

###Fixes###

NET VPN IDS: Have the customer provide IDS capabilities for the VPN implementation.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes:

NET1840 CAT: 3 Contract to company site VPNs are not implemented

Router Type:

Target(s): VPN

8500.2 IA Control: ECSC-1

Category: 4.2 - VPN

Condition(s): VPN

Vulnerability The SA and the IAO/NSO will ensure that if VPN technology is used to connect to a DOD network, the VPN client and concentrator are configured to deny the use of split tunneling when the connection originates from outside of the protected enclave.

The remote user will enter into a written agreement with the DOD site that allows the site to maintain administrative oversight and control privileges of the computer.

The remote user will ensure all communication to/from the site network employs security using FIPS 140-2 validated encryption such as AES, 3DES, SSH, or SSL.

Vulnerability Discussion: To provide the maximum level of security for both the DoD network and the remote corporate enterprise, the contractor will have to exceed the normal protection deployed on DoD workstations.

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks/Fixes: ###Checks###

NET VPN Contractor PC: Interview the IAO/NSO and examine the configuration of a VPN client.

Interview the IAO/NSO to verify compliance.

Interview the IAO/NSO to verify compliance.

###Fixes###

NET VPN Contractor PC: Ensure the contractor machine is secured with the appropriate STIG.

Ensure the contractor machine is updated with the latest virus engine and signature files.

Ensure the contractor machine employ a DoD-CERT approved firewall.

Ensure the contractor machine employ, at a minimum, a FIPS-140-2 encryption algorithm.

OPEN: ☐ **NOT A FINDING:** ☐ **NOT REVIEWED:** ☐ **NOT APPLICABLE:** ☐

Notes: